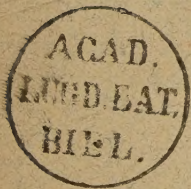


THE ANALYTIC REPRESENTATION OF SUBSTITUTIONS ON A POWER OF A PRIME NUMBER OF LETTERS WITH A DISCUSSION OF THE LINEAR GROUP.

A DISSERTATION PRESENTED TO THE FACULTY OF ARTS,
LITERATURE, AND SCIENCE, OF THE UNIVERSITY OF
CHICAGO, IN CANDIDACY FOR THE
DEGREE OF DOCTOR OF
PHILOSOPHY.

By
LEONARD EUGENE DICKSON.



Reprinted from the Annals of Mathematics, 1897.

THE ANALYTIC REPRESENTATION OF SUBSTITUTIONS ON A POWER OF A PRIME NUMBER OF LETTERS WITH A DIS- CUSSION OF THE LINEAR GROUP.*

By DR. LEONARD EUGENE DICKSON, Chicago, Ill.

TABLE OF CONTENTS.

Preface with literature.

PART I.—ANALYTIC REPRESENTATION OF SUBSTITUTIONS.

SECTION I.—*General Theory.*

- Arts. 1- 2. Definitions.
 3. Uniqueness of representation.
 4- 5. Lagrange's interpolation formula.
 6- 7. De Polignac's result anticipated.
 8. Matrix property of substitution quantic.
 9-11. Generalization of Hermite's Theorem.
 12. Reciprocal of a substitution quantic.
 13-15. Residue of a multinomial coefficient (mod p).
 16. Reduced form of substitution quantic.
 17. Degree not a divisor of $p^n - 1$.
 18. ξ^k a substitution quantic if k is prime to $p^n - 1$.

SECTION II.—*Quantics of degree prime to p .*

- 20-45. Complete determination of reduced quantics of degree ≤ 6 suitable on p^n letters.
 46-50. Preliminary study of septics.
 51-56. Quantics with an infinite range of suitability.

SECTION III.—*Quantics of degree a power of p .*

- 57-59. Quantics with all exponents powers of p .
 60-68. General theorems on quantics of degree p^r .
 69-74. Determination of all reduced $SQ[p^r; p^n]$, for $p^r \leq 7$ and partially for $p^r = 11$.
 75-77. General types of $SQ[p^r; p^n]$.

SECTION IV.—*Degree a multiple, not a power, of p .*

- 78-82. Determination of all reduced $SQ[6; 3^n]$.
 82-86. Special results on $SQ[6; 2^n]$.

Miscellany.

87. Table of all reduced $SQ[k; p^n]$, $k \leq 6$.
 88-89. Analytic generators of substitutions on 7 and 5 letters.
 90. Enumerative proof of Wilson's theorem.

* Dissertation accepted by the University of Chicago in partial fulfilment of the requirement for the degree Doctor of Philosophy.

PART II.—LINEAR GROUP.

SECTION I.—*Linear homogeneous group.*

1. Definition of a linear homogeneous substitution.
2. Literal and analytic composition; group.
3. Restriction to prime modulus.
4. Order of linear homogeneous group.
5. Transformation of indices; determinant invariant.
- 6–7. Decomposition of a linear homogeneous substitution.
- 8–12. Factors of composition of linear homogeneous group.
13. A triply infinite system of simple groups.

SECTION II.—*Linear fractional group.*

14. Definition, exhibition, and order.
15. Group of linear fractional substitutions with determinant unity is *simple*.
- 16–17. Remarks on systems of simple groups.

SECTION III.—*The Betti-Mathieu group.*

- 18–19. Identification with the linear group.
20. Order of the group.
- 21–24. Mathieu's special type of substitutions.

PREFACE.

This paper is an application of the Galois Field theory, a conception of fundamental importance in Higher Algebra. This theory is here presupposed and will be used in the abstract form given it by E. H. Moore.¹ Reference may also be made to Galois,² Serret³, Jordan⁴, Borel et Drach⁵, in a note by the latter the Galois Field being developed in its abstract form.

The aim in Part I is two-fold: (1) the complete determination of all quantics up to as high a degree as practicable which are suitable to represent substitutions on p^n letters, p being a prime, n an integer; (2) the determination of special quantics suitable on p^n letters, where for each quantic the combination (p, n) takes infinitely many values.

It is a remarkable fact that, on the one hand, the conditions necessary and sufficient to determine a substitution quantic are found by multinomial expansions,—on the other hand, one of the observed types of substitution quantics having an infinite range of suitability is a multinomial expansion

¹ Moore, *Proceedings of the Congress of Mathematics of 1893, at Chicago*.

² Galois, *Bulletin des Sciences mathématiques* de M. Férussac, vol. 13, p. 428, 1830; reprinted in Liouville's *Journal de Mathématiques*, vol. 11, pp. 398–407, 1846.

³ Serret, *Algèbre supérieure*, fifth edition, vol. 2, pp. 122–189.

⁴ Jordan, *Traité des substitutions*, pp. 14–18.

⁵ Borel et Drach, *Théorie des Nombres et Algèbre supérieure*, 1895, pp. 42–50, 58–62; Note, pp. 343–350.

(multiplied by a power of the variable) and the other type a reverse-binomial expansion (see §§ 53-54).

The results of this investigation warrant the conjecture that there exist a small number of types of substitution quantics of such wide ranges that together they represent all the $p^n!$ substitutions on p^n letters. Examples where apparently isolated quantics fall under a general type (when it is not *reduced*) are given in § 77.

While the aim in Part II* is primarily to generalize the work of Jordan on the linear homogeneous group, the treatment has been considerably modified to render the subject more accessible. The desire being chiefly non-cyclic simple groups, the modulus is supposed prime, which affords much simplification. On the other hand, many amplifications occur and also the correction of several errors (indicated by foot-notes).

In the same investigation there may occur marks of the Galois Fields of orders p^1 , p^n , and p^{mn} , $n > 1$, $m > 1$, when (as a useful notation) we use small Roman, small Greek, and capital Roman letters respectively.

Literature on the analytic representation of substitutions:

M. Hermite, *Sur les fonctions de sept lettres*, *Comptes Rendus des Séances de L'Académie des Sciences*, vol. 57, pp. 750-757, 1863.

Hermite's results (in whole or part) are given by:

Serret, *Cours D'Algèbre supérieure*, vol. 2, pp. 383-389 and 405-412;

Netto, *Substitutionentheorie*, ch. 8;

Jordan, *Traité des Substitutions*, pp. 88-91;

Borel et Drach, *Théorie des Nombres et Algèbre supérieure*, pp. 305-307, 1895.

Enrico Betti, *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo*, *Annali di Scienze Matematiche e Fisiche*, vol. 2, pp. 5-19, 1851; *Sulla risoluzione delle Equazioni algebriche*, *ibid*, vol. 3, pp. 49-115, 1852; *Sopra la teorica delle sostituzioni*, *ibid*, vol. 6, pp. 5-34, 1855.

Émile Mathieu, *Mémoire sur le nombre de valeurs que peut acquérir une fonction quand on y permute ses variables de toutes les manières possibles*, *Journal de Mathématiques pure et appliquées*, second series, vol. 5, pp. 9-42, 1860; *Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, *ibid*, vol. 6, pp. 241-323, 1861.

F. Brioschi. *Des substitutions de la forme*

$$\theta(r) = e(r^{n-2} + ar^{\frac{n-3}{2}})$$

* For the suggestion of this generalization as leading to a triply infinite system of simple groups, as also for much valuable aid throughout the investigation, I am indebted to Professor Moore.

pour un nombre n premier de lettres, *Mathematische Annalen*, vol. 2, pp. 467–470, 1870.

De Polignac, *Sur la représentation analytique des substitutions*, *Bulletin de la Société Mathématique de France*, vol. 9, pp. 59–67, 1881.

A. Grandi, *Un teorema sulla rappresentazione analitica delle sostituzioni sopra un numero primo di elementi*, *Giornale Matematico* del Prof. G. Battaglini, vol. 19, pp. 238–245. The conditions are found under which

$$x^{p-s} + ax^{\frac{p+s+1}{2}} + bx$$

shall represent a substitution on p letters. A generalization by the same writer is given in *Reale Istituto Lombardo di scienze e lettere, Rendiconti*, Milano, vol. 16, pp. 101–111. For abstracts of each see *Fortschritte der Mathematik*, vol. 13, p. 118, 1881, and vol. 15, p. 116, 1883.

J. L. Rogers, *On the Analytical Representation of Heptagrams*, *London Mathematical Society*, vol. 22, pp. 37–52, 1890.

L. E. Dickson, *Analytic Functions Suitable to Represent Substitutions*, *American Journal of Mathematics*, vol. 18, pp. 210–218, 1896.

PART I.—ANALYTIC REPRESENTATION OF SUBSTITUTIONS ON A POWER OF A PRIME NUMBER OF LETTERS.

SECTION I.—General Theory.

1. Let ξ be any mark of the Galois Field of order p^n , p being a prime and n a positive integer. Also let $\varphi(\xi)$ be an integral function of ξ having as coefficients certain marks of the $GF[p^n]$. The replacing of the letter l_ξ by the letter $l_{\varphi(\xi)}$ defines a *substitution* on p^n letters, in notation,

$$\xi' = \varphi(\xi).$$

2. In order that $\varphi(\xi)$ shall indeed be suitable to represent a substitution on the marks

$$\mu_i \quad (i = 0, 1, \dots, p^n - 1),$$

it is necessary and sufficient that $\varphi(\mu_0), \varphi(\mu_1), \dots, \varphi(\mu_{p^n-1})$, be identical with $\mu_0, \mu_1, \dots, \mu_{p^n-1}$, except as to order. If an integral function of degree k belonging to the $GF[p^n]$ satisfies these conditions, it will be called a *substitution quantic* of degree k on p^n letters and denoted thus

$$SQ[k; p^n].$$

The degree k will be supposed $< p^n$ owing to the equation

$$\xi^{p^n} = \xi,$$

satisfied by every mark of the field.

3. Theorem. *Two different quantics $\varphi(\xi)$ and $\psi(\xi)$ belonging to the $GF[p^n]$ cannot represent the same literal substitution.*

For if the substitution replace the index μ_i by μ_{a_i} for $i = 0, 1, \dots, p^n - 1$, then must

$$\varphi(\mu_i) = \mu_{a_i} = \psi(\mu_i) \quad (i = 0, 1, \dots, p^n - 1).$$

Thus

$$\varphi(\xi) - \psi(\xi) = 0$$

is of degree $p^n - 1$ at most but has p^n distinct roots μ_i . It is thus an identity in ξ .

4. The most evident substitution quantic is the integral function $\varphi(\xi)$ which gives Lagrange's interpolation formula:

$$\varphi(\xi) = \sum_{i=0}^{p^n-1} \frac{\mu_{a_i} F(\xi)}{(\xi - \mu_i) F'(\mu_i)} \quad (1)$$

where $a_0, a_1, \dots, a_{p^n-1}$ is any permutation of $0, 1, \dots, p^n - 1$, and where

$$F(\xi) = \prod_{i=0}^{p^n-1} (\xi - \mu_i),$$

and F' denotes its derivative. Thus

$$\xi' = \varphi(\xi)$$

represents the substitution

$$\begin{bmatrix} \mu_0 & \mu_1 & \dots & \mu_{p^n-1} \\ \mu_{a_0} & \mu_{a_1} & \dots & \mu_{a_{p^n-1}} \end{bmatrix}.$$

5. Following Hermite's method* for the case $n = 1$, we may give (1) a simpler form.

In the $GF[p^n]$,

$$F(\xi) = \xi^{p^n} - \xi; \quad F'(\xi) = -1.$$

$$\varphi(\xi) = - \sum_{i=0}^{p^n-1} \frac{\mu_{a_i} (\xi^{p^n} - \xi)}{\xi - \mu_i}.$$

Taking $\mu_0 = 0$, so that

$$\mu_i^{p^n-1} - 1 = 0 \quad (i = 1, 2, \dots, p^n - 1)$$

* Cf. Serret, l. c. 2, pp. 384-5.

and performing the division by $\xi - \mu_i$,

$$\varphi(\xi) \equiv -\mu_{a_0}(\xi^{p^n-1} - 1) - \sum_{i=1}^{p^n-1} \mu_{a_i}(\xi^{p^n-1} + \mu_i \xi^{p^n-2} + \dots + \mu_i^{p^n-2} \xi).$$

Arranging according to powers of ξ and noting that*

$$\mu_{a_0} = - \sum_{i=1}^{p^n-1} \mu_{a_i},$$

we reach the desired quantic,

$$\varphi(\xi) \equiv \sum_{j=0}^{p^n-2} a_j \xi^j \quad (2)$$

where

$$a_j = - \sum_{i=0}^{p^n-1} \mu_{a_i} \cdot \mu_i^{p^n-1-j} \quad (j = 0, 1, \dots, p^n-2). \quad (3)$$

It follows from § 3 that every substitution quantic on p^n letters which belongs to the $GF[p^n]$ is contained in the form (2).

6. The conditions on a_j that an arbitrary quantic

$$\varphi(\xi) \equiv \sum_{j=0}^{p^n-1} a_j \xi^j$$

belonging to the $GF[p^n]$ shall represent a substitution on its p^n marks μ_i are

$$\sum_{j=0}^{p^n-1} a_j \mu_i^j = \varphi(\mu_i) \quad (i = 0, 1, \dots, p^n-1), \quad (4)$$

where $\varphi(\mu_i) \equiv \mu_{a_i}$ form a permutation of μ_i . Applying the lemma proven in § 10, we have on adding the p^n equations (4),

$$-a_{p^n-1} = \sum_{i=0}^{p^n-1} \varphi(\mu_i) = 0.$$

Taking a_{p^n-1} zero and dropping the first one of the equations (4), we have the system of conditions

$$\sum_{j=0}^{p^n-2} a_j \mu_i^j = \varphi(\mu_i) \quad (i = 1, 2, \dots, p^n-1). \quad (4')$$

The determinant†

$$|\mu_i^j| = \Pi(\mu_r - \mu_s) \neq 0,$$

where $r, s = 1, 2, \dots, p^n-1, r > s$.

We may thus express a_j linearly in terms of μ_{a_i} . By equation (2) of § 5, this is done by formula (3).

* $\sum_{i=0}^{p^n-1} \mu_{a_i} = \sum_{i=0}^{p^n-1} \mu_i = 0$ by § 10.

† Baltzer, *Theorie und Anwendung der Determinanten*, p. 85.

7. The gist of De Polignac's paper is to actually solve equations (4) for the case $n = 1$. Using a and m for the integers corresponding to the marks α and μ , his result is given in the form

$$a_j = \sum_{i=1}^{p-2} \{(-1)^j - i^{p-1-j}\} m_{\alpha_i},$$

where previously m_{α_0} has been taken to be zero. Subtracting

$$(-1)^j \cdot \sum_{i=1}^{p-1} m_{\alpha_i} \equiv 0 \pmod{p},$$

$$a_j = -(-1)^j m_{\alpha_{p-1}} - \sum_{i=1}^{p-2} i^{p-1-j} m_{\alpha_i} = - \sum_{i=1}^{p-1} i^{p-1-j} m_{\alpha_i}. \quad (3_{n=1})$$

8. We may independently verify the inverse character of the linear relations (3) and (4) between the coefficients a_j of any substitution quantic $\varphi(\xi)$ and the marks $\varphi(\mu_i) \equiv \mu_{\alpha_i}$. By (4') the matrix

$$\begin{bmatrix} 1, & \mu_1, & \mu_1^2, & \dots, & \mu_1^{p^n-2} \\ 1, & \mu_2, & \mu_2^2, & \dots, & \mu_2^{p^n-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & \mu_{p^n-1}, & \mu_{p^n-1}^2, & \dots, & \mu_{p^n-1}^{p^n-2} \end{bmatrix}$$

expresses $\varphi(\mu_1), \varphi(\mu_2), \dots, \varphi(\mu_{p^n-1})$ linearly in terms of $\alpha_0, \alpha_1, \dots, \alpha_{p^n-2}$. Inversely, by (3) the matrix

$$\begin{bmatrix} -1, & -1, & \dots, & -1 \\ -\mu_1^{p^n-2}, & -\mu_2^{p^n-2}, & \dots, & -\mu_{p^n-1}^{p^n-2} \\ -\mu_1^{p^n-3}, & -\mu_2^{p^n-3}, & \dots, & -\mu_{p^n-1}^{p^n-3} \\ \cdot & \cdot & \cdot & \cdot \\ -\mu_1, & -\mu_2, & \dots, & -\mu_{p^n-1} \end{bmatrix}$$

expresses the latter linearly in terms of the former. To prove that the product of the two matrices is the identity, let c^{ij} denote the term in the product derived from the i th row of the first and the j th column of the second matrix. Then

$$c_{ij} = -1 - \mu_i \mu_j^{p^n-2} - \mu_i^2 \mu_j^{p^n-3} - \dots - \mu_i^{p^n-2} \mu_j.$$

Thus

$$c_{ii} = -(p^n - 1) = +1 \quad (i = 1, 2, \dots, p^n - 1).$$

For $i, j = 1, 2, \dots, p^n - 1$, but $i \neq j$,

$$1 = \frac{\mu_i^{p^n} - \mu_j^{p^n}}{\mu_i - \mu_j} = \mu_i^{p^n-1} + \mu_i^{p^n-2} \mu_j + \dots + \mu_i \mu_j^{p^n-2} + \mu_j^{p^n-1}.$$

Hence $c_{ij} = 0$ if $i \neq j$.

From the matrix expressing $\varphi(\mu_i)$ in terms of $\alpha_0, \alpha_1, \dots, \alpha_{p^n-2}$, we derive by reflection on its main diagonal and change of sign of all its elements a matrix which expresses $\alpha_0, \alpha_{p^n-2}, \alpha_{p^n-3}, \dots, \alpha_1$ in terms of

$$\varphi(\mu_i) \quad (i = 1, 2, \dots, p^n - 1).$$

9. Lemma. $\mu_0, \mu_1, \dots, \mu_{p^n-1}$, being the marks of the $GF[p^n]$ and t a positive integer,

$$\sum_{i=0}^{p^n-1} \mu_i^t = \begin{cases} 0 & \text{for } t < p^n - 1 \\ -1 & \text{for } t = p^n - 1 \end{cases}$$

For let σ_t denote the sum of the t th powers of the roots of the equation belonging to the $GF[p^n]$

$$\sum_{i=0}^{p^n} y_i \xi^{p^n-i} = 0 \quad (y_0 = 1). \quad (5)$$

Applying Newton's identity (as is allowable)

$$\sigma_k + y_1 \sigma_{k-1} + y_2 \sigma_{k-2} + \dots + y_{k-1} \sigma_1 + k y_k = 0. \quad (k = 1, \dots, p^n)$$

If for (5) we take the equation whose roots are μ_i ,

$$\xi^{p^n} - \xi = 0$$

the proof of the lemma follows.

10. Lemma. If, in the notation of § 9,

$$\sigma_{p^n-1} \neq 0, \sigma_t = 0 \quad \begin{cases} t = 1, 2, \dots, p^n - 2 \\ t \neq 0, (\text{mod } p) \end{cases},$$

and if all the roots of equation (5) be marks of the $GF[p^n]$, then will (5) take the form

$$\xi^{p^n} + y_{p^n-1} \xi + y_{p^n} = 0.$$

Applying Newton's identity cited above, we find

$$y_i = 0 \quad \begin{cases} i = 1, 2, \dots, p^n - 2 \\ i \neq 0 \pmod{p} \end{cases},$$

$$\sigma_p = \sigma_{2p} = \dots = \sigma_{p^n-p} = \sigma_{p^n} = 0.$$

To determine $y_p, y_{2p}, \dots, y_{p^n-p}$ apply the identity

$$\sigma_k + y_1 \sigma_{k-1} + y_2 \sigma_{k-2} + \dots + y_{p^n} \sigma_{k-p^n} = 0 \quad (k \geq p^n),$$

which reduces to

$$\sigma_k + y_p \sigma_{k-p} + y_{2p} \sigma_{k-2p} + \dots + y_{p^{n-1}} \sigma_{k-p^{n-1}} + y_{p^n} \sigma_{k-p^n} = 0.$$

By our assumption on the roots,

$$\sigma_t = \sigma_{t+p^{n-1}}.$$

Hence for $k = p^n + p - 1$,

$$y_p \sigma_{p-1} = 0.$$

Generally, for $k = p^n + lp - 1$, $l \leq p^{n-1} - 1$,

$$y_l^p \sigma_{p^{n-1}-1} = 0.$$

Since $\sigma_{p^{n-1}} \neq 0$ by hypothesis, $y_{lp} = 0$.

11. Generalization of Hermite's Theorem.

The necessary and sufficient conditions that $\varphi(\xi)$ shall be suitable to represent a substitution on p^n letters are :

(1) Every t th power of $\varphi(\xi)$, for $t < p^n - 1$ and prime to p , shall reduce to a degree $\leq p^n - 2$ when we lower the exponents of ξ below p^n by means of the equation

$$\xi^{p^n} - \xi = 0;$$

(2) There shall be but one distinct root of

$$\varphi(\xi) = 0.$$

Proof : Suppose

$$\varphi(\xi) = \sum_{i=0}^{p^n-1} a_i \xi^i.$$

After reducing exponents below p^n let

$$[\varphi(\xi)]^m = \sum_{i=0}^{p^n-1} a_i^{(m)} \xi^i.$$

Give to ξ the values of the p^n marks μ_j of the field and add the resulting equalities.

$$\sum_{j=0}^{p^n-1} [\varphi(\mu_j)]^m = p^n a_0^{(m)} + a_1^{(m)} \sum_{j=0}^{p^n-1} \mu_j + \dots + a_{p^n-1}^{(m)} \sum_{j=0}^{p^n-1} \mu_j^{p^n-1}.$$

Hence by § 9, for $m < p^n - 1$,

$$\sum_{j=0}^{p^n-1} [\varphi(\mu_j)]^m = a_{p^n-1}^{(m)}.$$

But if $\varphi(\xi)$ represents a substitution,

$$\sum_{j=0}^{p^n-1} [\varphi(\mu_j)]^m = \sum_{j=0}^{p^n-1} \mu_j^m = 0$$

if $m < p^n - 1$. Hence a necessary condition is

$$a_{p^n-1}^{(m)} = 0. \quad (m = 1, 2, \dots, p^n - 2)$$

Also there must be one and only one of the marks $\varphi(\mu_j)$ equal to zero, i. e. but one distinct root of $\varphi(\xi) = 0$.

Inversely, suppose (1) and (2) are satisfied, so that

$$\begin{aligned} \sum_{j=0}^{p^n-1} [\varphi(\mu_j)]^t &= -a_{p^n-1}^{(t)} = 0 & \left[\begin{array}{l} t = 1, 2, \dots, p^n - 2 \\ t \not\equiv 0 \pmod{p} \end{array} \right] \\ \sum_{j=0}^{p^n-1} [\varphi(\mu_j)]^{p^n-1} &= -1 \neq 0. \end{aligned}$$

Then by § 10 the equation

$$\prod_{j=0}^{p^n-1} [\eta - \varphi(\mu_j)] = 0$$

takes the form

$$\eta^{p^n} + y_{p^n-1} \eta + y_{p^n} = 0$$

or

$$\eta(1 + y_{p^n-1}) + y_{p^n} = 0.$$

If $y_{p^n-1} \neq -1$, this linear equation is satisfied by the p^n marks $\varphi(\mu_j)$. These must therefore be equal, and since their sum is zero, each must be zero. But in this case the equation belonging to our field,

$$\varphi(\xi) = \sum_{i=0}^{p^n-2} a_i \xi^i = 0$$

would have p^n distinct roots $\xi = \mu_i$ ($i = 0, 1, \dots, p^n - 1$) which is impossible. Hence $y_{p^n-1} = -1$ and then, since one of the $\varphi(\mu_j)$'s are zero, $y_{p^n} = 0$. Thus the marks $\varphi(\mu_j)$ are identical apart from order to the roots μ_i of

$$\eta^{p^n} - \eta = 0.$$

12. Reciprocal* of a substitution quantic. Given a substitution quantic

$$\eta = \varphi(\xi) = \sum_{i=1}^{p^n-2} a_i \xi^{p^n-1-i}.$$

* Rogers, l. c. for $p^n = 7$. His proof is objectionable, since he makes $\xi^6 = 1 \pmod{7}$ while ξ is to be taken $= 0$.

Suppose its reciprocal is

$$\xi = \sum_{i=1}^{p^n-2} \beta_i \eta^{p^n-1-i}.$$

Then

$$\xi \eta^t = \xi [\varphi(\xi)]^t = \sum_{i=1}^{p^n-1} a_i^{(t)} \xi^{p^n-i},$$

after reduction of exponents as in § 11. On the other hand,

$$\xi \eta^t = \sum_{i=1}^{p^n-2} \beta_i \eta^{p^n-1-i+t} = \beta_1 \eta^{t-1} + \beta_2 \eta^{t-2} + \dots + \beta_i \eta^{p^n-1} + \dots + \beta_{p^n-2} \eta^{t+1}.$$

Since $\eta = \varphi(\xi)$ is a $SQ[; p^n]$, then η^j contains no term ξ^{p^n-1} as long as $j < p^n - 1$. Hence the term $a_1^{(t)} \xi^{p^n-1}$ must be derived from $\beta_i \eta^{p^n-1}$. But $\eta = 0$ if and only if $\xi = 0$, so that $\eta^{p^n-1} = \xi^{p^n-1}$. Hence

$$\beta_t = a_1^{(t)}$$

or β_t is the coefficient of ξ^{p^n-2} in $[\varphi(\xi)]^t$.

Residue of a multinomial coefficient modulo p , p being prime, §§ 13-15.

13. A number m can be written in one and but one way in the form

$$m = \sum_{i=0}^n a_i^{(m)} p^i,$$

where $a_i^{(m)}$ is zero or a positive integer $< p$. Then,* if P_m denotes the highest power of p which divides $m!$, we have

$$P_m = (m - \sum_{i=0}^n a_i^{(m)}) / (p - 1).$$

14. Theorem. The multinomial coefficient

$$\frac{m!}{m_1! m_2! \dots m_t!},$$

where $m_1 + m_2 + \dots + m_t = m$, is prime to p if and only if, when each m_k is written in the form

$$m_k = \sum_{i=0}^n a_i^{(m_k)} p^i,$$

we have as numerical equalities

$$\sum_{k=1}^t a_i^{(m_k)} = a_i^{(m)} \quad (i = 0, 1, \dots, n).$$

* Bachmann, *Zahlentheorie*, I, p. 33.

Proof.—The necessary and sufficient condition is

$$P_m = P_{m_1} + P_{m_2} + \dots + P_{m_t},$$

or

$$\sum_{i=0}^n a_i^{(m)} = \sum_{i=0}^n a_i^{(m_1)} + \sum_{i=0}^n a_i^{(m_2)} + \dots + \sum_{i=0}^n a_i^{(m_t)}.$$

It follows that if m (written in the above form) be partitioned into $m_1 + m_2 + \dots + m_t$, the partitioning must take place in the coefficients $a_i^{(m)}$ of the powers of p each independently of the others.

Example. $42 = 2^5 + 2^3 + 2$; hence the binomial coefficient c_k^{42} is *odd* only if $k = 2, 2^3, 2 + 2^3, 2^5, 2 + 2^5, 2^3 + 2^5, 2 + 2^3 + 2^5$.

15. Theorem. If the multinomial coefficient be prime to p , it is congruent modulo p to

$$\prod_i \frac{a_i^{(m)}!}{a_i^{(m_1)}! a_i^{(m_2)}! \dots a_i^{(m_t)}!}$$

where $s! = 1$, if $s = 0$.

In proof let

$$m = pq_1 + r_1, q_1 = pq_2 + r_2, \text{ etc.,}$$

where $r_1, r_2, \dots$ are positive integers $< p$. Then

$$\begin{aligned} m! &= (1 \cdot 2 \cdot 3 \dots p-1) p (p-1 \cdot p-2 \dots 2p-1) 2p \dots \\ &\quad q_1 p (q_1 p + 1 \dots q_1 p + r_1) \\ &\equiv (\overline{p-1})^{q_1} p^{q_1} \cdot q_1! r_1! \pmod{p} \\ &\equiv (-p)^{q_1} \cdot q_1! r_1!. \end{aligned}$$

Similarly,

$$q_1! \equiv (-p)^{q_2} \cdot q_2! r_2! \pmod{p}, \text{ etc.}$$

Hence

$$m! \equiv (-p)^{\sum q_i} \prod_i (r_i!).$$

But if $E(s)$ denotes the greatest integer in s ,

$$\sum_i q_i = \sum_i E(m/p^i) = P_m^*.$$

Thus

$$m! \equiv (-p)^{P_m} \prod_i a_i^{(m)}!$$

Proceeding likewise for $m_1!, m_2!, \dots, m_t!$ and applying § 14, we have the proof of the theorem.

16. *Reduced form of substitution quantics.* Let $\varphi(\xi) = a_0 \xi^k + a_1 \xi^{k-1} + \dots$ be a $SQ[k; p^n]$. If on the right and left of the substitution

$$\xi' = \varphi(\xi)$$

* Bachmann, *Zahlentheorie*, p. 32.

we apply linear substitutions of the form

$$\xi' = \beta_1 \xi + \beta_2 \quad (\beta_1 \neq 0)$$

we obtain a substitution

$$\xi' = \beta_1 \varphi(\beta_1' \xi + \beta_2') + \beta_2 = \varphi_1(\xi).$$

Take $\beta_1' = 1$ and dispose of the indeterminate β_1 so that the coefficient of ξ^k in $\varphi_1(\xi)$ shall be unity. If $a_1 \neq 0$, the coefficient $k\beta_2' + \beta_1 a_1$ of ξ^{k-1} in $\varphi_1(\xi)$ can, by choice of β_2' , be made zero, if and only if k be prime to p . Finally β_2 is chosen to make the constant term zero. Then $\varphi_1(\xi)$, in which the coefficient of ξ^k is unity, the constant term zero, and when k is prime to p the coefficient of ξ^{k-1} zero, will be called the *reduced form** of $\varphi(\xi)$ for the $GF[p^n]$.

17. Theorem. $\xi^k + a_1 \xi^{k-1} + a_2 \xi^{k-2} + \dots + a_{k-1} \xi$ is not a substitution quantic on p^n marks if p^n be of the form $mk + 1$, $k > 1$. For on raising it to the power $(p^n - 1)/k$ the coefficient of ξ^{p^n-1} is $1 \neq 0$.

18. Theorem. ξ^k is a $SQ[k; p^n]$ if and only if k be relatively prime to $p^n - 1$.

For, l being any integer $< p^n - 1$ and prime to p , lk must not be a multiple of $p^n - 1$ (by § 11).

Corollary.—The extraction of k th roots in the $GF[p^n]$ is *always* possible (and then uniquely) if and only if k be prime to $p^n - 1$.

SECTION II.—Degree k prime to p .

19. Using the same method as in my paper† giving a complete list of $SQ[k; p^n]$ for $k < 7$ and p any prime, I shall first determine all $SQ[k; p^n]$ for $k < 7$, p any prime not a divisor of k , and n any integer. After a preliminary study of septics, I shall conclude Section II with the derivation of a remarkable class of substitution quantics of arbitrary odd degree k .

Complete determination of reduced quantics of degree $k < 7$ suitable to represent substitutions on p^n letters, p being prime not a divisor of k , §§ 20–45.

20. ξ is suitable for every p^n .

21. ξ^2 is the reduced quadratic and is rejected by § 17 since p^n is odd.

22. $\xi^3 + a\xi$.

(a) The case p^n of the form $3m + 1$ is rejected by § 17.

(b) The case $p^n = 3m + 2$.

Then $(\xi^3 + a\xi)^{m+1}$ gives $(m + 1)a$ as the coefficient of ξ^{3m+1} . Hence, by

* By making use of the indeterminate β_1' a further reduction may often be made in $\varphi_1(\xi)$. The simplest form thus obtainable is called *ultimately reduced*. Thus $\xi^4 \pm 3\xi$ reduce to $\xi^4 + 3\xi$.

† *American Journal of Mathematics*, Vol. 18, pp. 210–218, 1896.

§ 11, $a = 0$; for if $m + 1$ were divisible by p , then would also $3m + 3$ or $p^n + 1$. The remaining form ξ^3 is suitable by § 18.

$$23. \xi^4 + a\xi^2 + \beta\xi.$$

The only case to consider here is $p^n = 4m + 3$.

The $m + 1$ st power requires $(m + 1)a = 0$ or $a = 0$.

$(\xi^4 + \beta\xi)^{m+2}$ requires $\frac{(m+2)(m+1)}{2}\beta^2 = 0$, provided $p^n > 7$. Hence

$\beta = 0$; for if $m + 2$ be divisible by p then is also $4m + 8$ or $p^n + 5$, i. e. $p = 5$, while p must be of the form $4l + 3$.

But ξ^4 is rejected by § 18, viz, by the power $l = 2m + 1$.

For the case above excluded, $p = 7$, $n = 1$, we have Hermite's result, the suitable quartics $\xi^4 \pm 3\xi$.

Reduced quintic $\xi^5 + a\xi^3 + \beta\xi^2 + \gamma\xi$, §§ 24-44.

24. The case $p^n = 5m + 2$. Hence n is odd.

The power $m + 1$ requires

$$(m + 1)\gamma + \frac{(m + 1)m}{2}a^2 = 0.$$

But $m + 1$ is divisible by p only if $p = 3$. Thus if $p \neq 3$,

$$5\gamma = a^2. \quad (1)$$

The power $m + 2$ requires if $p^n > 7$

$$\frac{(m+2)(m+1)m}{1 \cdot 2 \cdot 3} \{6a\beta\gamma + \beta^3 + (m-1)a^3\beta\} = 0.$$

Hence if $p \neq 2$ and $p^n > 7$,

$$5(6a\beta\gamma + \beta^3) - 7a^3\beta = 0. \quad (2)$$

From (1) and (2), if $p \neq 2$ and $\neq 3$ and if $p^n \neq 7$,

$$5\beta^3 = a^3\beta. \quad (3)$$

The power $m + 3$ requires if $p^n > 7$

$$c_4^{m+3} \left\{ 4a\gamma^3 + 6\beta^2\gamma^2 + \frac{m-1}{5}(10a^3\gamma^2 + 30a^2\beta^2\gamma + 5a\beta^4) \right. \\ \left. + \frac{(m-1)(m-2)}{5 \cdot 6}(6a^5\gamma + 15a^4\beta^2) + \frac{(m-1)(m-2)(m-3)}{5 \cdot 6 \cdot 7}a^7 \right\} = 0.$$

Now $m + 3$ is divisible by p only if $p = 13$. Hence if p is neither 2 nor 13 we may divide off the binomial factor c_4^{m+3} . Multiplying the resulting equa-

tion by 5^4 , replacing $5(m-1)$ by -7 , etc., we have for p^n not $2^n, 7^1, 13^n$ the condition

$$20a(5\gamma)^3 + 150\beta^2(5\gamma)^2 - 70a^3(5\gamma)^2 - 1050a^2\beta^2(5\gamma) - 875a\beta^4 + 84a^5(5\gamma) + 1050a^4\beta^2 - 34a^7 = 0. \quad (4)$$

Applying (1) to (4):

$$150a^4\beta^2 - 875a\beta^4 = 0,$$

from which by (3) we find $\beta = 0$.

For the proof that the resulting form

$$5\tilde{\xi}^5 + 5a\tilde{\xi}^3 + a^2\tilde{\xi}$$

does represent a substitution on $p^n = 5m \pm 2$ letters, a being arbitrary, see § 39.

25. The case $p^n = 13^n = 5m + 2$.

The powers $m+3, m+4, m+5$ give identities. The power $m+6$ requires

$$c_{14}^{m+6} \cdot 14a^3\beta = 0 \text{ or } a^3\beta = 0.$$

For, $5m+2 \equiv 0 \pmod{13}$ i. e. $m \equiv 10 \pmod{13}$. Thus c_k^{m+6} or c_k^{13t+8} is $\neq 0$ only for $k = 1, 2, 3, 13, 14, 15, 16, 26, \dots$, by § 14.

It follows from this equation and (3) that $\beta = 0$.

26. The case $p = 7, n = 1$.

Hermite gave the complete list of suitable forms:

$$\tilde{\xi}^5 \pm 2\tilde{\xi}^2.$$

$$\tilde{\xi}^5 + a\tilde{\xi}^3 \pm \tilde{\xi}^2 + 3a^2\tilde{\xi}, a = \text{quadratic non-residue of } 7.$$

$$\tilde{\xi}^5 + a\tilde{\xi}^3 \pm 3a^2\tilde{\xi}, a = \text{arbitrary}.$$

The last may be written $5\tilde{\xi}^5 + 5a\tilde{\xi}^3 + a^2\tilde{\xi}$.

27. The case $p^n = 3^n = 5m + 2$.

The powers $m+2$ and $m+3$ require by (2) and (4)

$$2\beta^3 = a^3\beta \quad (2')$$

$$a\gamma^3 - a^3\gamma^2 + a\beta^4 - a^7 = 0. \quad (4')$$

Since $n \geq 3$, $5m+2 \equiv 0 \pmod{27}$ or $m \equiv 5 \pmod{27}$. Hence c_k^{m+6} or c_k^{27t+11} is $\neq 0$ only if $k = 1, 2, 9, 10, 11$, or ≥ 27 .

The power $m+6$ thus requires, if $n > 3$,

$$c_{10}^{m+6} \cdot 10a\beta^9 = a\beta^9 = 0. \quad (5')$$

Thus $\beta = 0$ and (4') becomes

$$a(\gamma + \alpha^2)(\gamma^2 + \gamma\alpha^2 - \alpha^4) = 0.$$

If $a \neq 0$, $\gamma = -\alpha^2$; for if the last factor vanishes,

$$(\gamma + \alpha^2)^2 = -\gamma^2,$$

while -1 is a not-square in the $GF[3^1]$ and hence in the $GF[3^n]$, n being odd.

If $a = 0$, the power $m + 9$ of $\xi^5 + \gamma\xi$ requires

$$c_{11}^{m+9}\gamma^{11} = \gamma^{11} = 0.$$

The possible form is thus $5\xi^5 + 5a\xi^3 + a^2\xi$ when $n > 3$.

28. The case $p^n = 3^3$.

The powers 11 and 13 require

$$\beta + a\beta^9 = 0 \quad * \quad (5'')$$

$$\beta^3\gamma + \beta\gamma^9 + \beta^9\gamma^3 + \beta^{13} = 0. \quad (6'')$$

Suppose $\beta \neq 0$. Then by (2'), $\beta^2 = -\alpha^3$, so that (5') is satisfied and (4') becomes

$$a\gamma^2(\gamma - \alpha^2) = 0.$$

But if either $\gamma = 0$ or $\gamma = \alpha^2$, (6'') requires that $\beta = 0$. Since $\beta = 0$ we have $\gamma = -\alpha^2$ as in the case $n > 3$.

29. The case $p^n = 2^n = 5m + 2$.

Since $n \geq 5$, $m \equiv 6 \pmod{32}$. The power $m + 5$ requires

$$c_8^{m+5} \cdot \beta^8 + c_{10}^{m+5} \cdot 45\alpha^8\gamma^2 + c_{11}^{m+5}(11\alpha^{10}\gamma + 55\alpha^9\beta^2) = 0.$$

Applying (1), $\gamma = \alpha^2$, this becomes

$$\beta^2(\beta^6 + \alpha^9) = 0. \quad (7)$$

The power $m + 7$ requires if $n > 5$,

$$a\gamma^8 + \alpha^5\beta^8 + \alpha^9\gamma^4 = 0.$$

Applying (1) this becomes $\alpha^5\beta^8 = 0$. Hence $\beta = 0$.

For $n = 5$, the 13th power requires a condition which on applying (1) becomes exactly the fourth power of (7).

For $n = 5$, the 15th power requires

$$\gamma^{11} + \beta^4\gamma^8 + \alpha^4\gamma^9 + \beta^8\gamma^5 + \alpha^6\gamma^8 + \alpha^2\beta^8\gamma^4 + \beta^{12}\gamma^2 + \alpha^8\gamma^7 + \alpha^4\beta^8\gamma^3 + \alpha^2\beta^{12}\gamma + \alpha\beta^{14} = 0.$$

Applying (1) this becomes

$$a\beta^4(a^{15} + a^9\beta^4 + \beta^{10}) = 0. \quad (8)$$

If $\beta \neq 0$, $\beta^6 = a^9$ by (7), whence (8) becomes $a^{15} = 0$. Hence must $\beta = 0$.

30. Summary of §§ 24-29. The only possible reduced substitution quintic on $p^n = 5m + 2$ letters is

$$5\xi^5 + 5a\xi^3 + a^2\xi, \quad a \text{ arbitrary,}$$

except for $p = 7$, $n = 1$ when we have two additional forms :

$$\begin{aligned} \xi^5 \pm 2\xi^2 \\ \xi^5 + a\xi^3 \pm \xi^2 + 3a^2\xi, \end{aligned}$$

where a is a quadratic non-residue of 7.

31. The case $p^n = 5m + 3$.

The power $m + 1$ requires $(m + 1)\beta = 0$. Hence if $p \neq 2$, $\beta = 0$. The power $m + 2$ of $\xi^5 + a\xi^3 + \gamma\xi$ requires

$$c_2^{m+2}\gamma^2 + c_3^{m+2} \cdot 3a^2\gamma + c_4^{m+2}a^4 = 0. \quad (1)$$

If $p \neq 7$ we may divide out c_2^{m+2} , giving readily

$$25\gamma^2 - 15a^2\gamma + 2a^4 = 0.$$

Hence, if $p \neq 2, \neq 7$, either $5\gamma = a^2$ or $5\gamma = 2a^2$.

The power $m + 4$ requires for $p^n > 13$,

$$c_5^{5m+4} \cdot 5a\gamma^4 + c_6^{m+4} \cdot 20a^3\gamma^3 + c_7^{m+4} \cdot 21a^5\gamma^2 + c_8^{m+4} \cdot 8a^7\gamma + c_9^{m+4}a^9 = 0. \quad (2)$$

If p is not 2, 3, 7 or 17, we may divide out $(m + 4)(m + 3)(m + 2)(m + 1)m$, multiply by $5^4 \cdot 7!$ and replace $5(m + 1)$ by -8 , etc., giving

$$210a(5\gamma)^4 - 8 \cdot 140a^3(5\gamma)^3 + 8 \cdot 13 \cdot 21a^5(5\gamma)^2 - 8 \cdot 13 \cdot 18a^7(5\gamma) + 23 \cdot 26a^9 = 0.$$

If $5\gamma = a^2$, this becomes

$$a^9(210 - 8 \cdot 140 + 8 \cdot 13 \cdot 21 - 8 \cdot 13 \cdot 18 + 23 \cdot 26) = 0,$$

in which the coefficient of a^9 is identically zero. If $5\gamma = 2a^2$, the coefficient of a^9 reduces to -10 . Hence in this case $a = \gamma = 0$.

Thus for p^n not $2^n, 3^n, 7^n, 17^n$ or 13, the only possible quintic on $p^n = 5m + 3$ letters is reducible to

$$5\xi^5 + 5a\xi^3 + a^2\xi.$$

32. For $p = 13$, $n = 1$, I have elsewhere* shown that the only suitable quintics are

$$\begin{aligned} 5\xi^5 & \mid 5a\xi^3 + a^2\xi, & a = \text{arbitrary.} \\ 5\xi^5 + 5a\xi^3 + 2a^2\xi, & a = \text{quadratic non-residue of 13.} \end{aligned}$$

33. The case $p^n = 17^n = 5m + 3$.

The value $5\gamma = 2a^2$ is rejected since the equation

$$5\xi^5 + 5a\xi^3 + 2a^2\xi = 0$$

has a solution $\neq 0$ for every a when $p = 17$. Thus

$$5\xi(\xi^4 + a\xi^2 - 3a^2) = 0$$

has the solutions $\xi^2 = 4a$ and $-5a$. Now -5 is a not-square in the $GF[17]$ and hence also in the $GF[17^n]$, n being odd. Thus whether a be a square or a not-square, we have a solution $\xi \neq 0$ belonging to the field.

34. The case $p^n = 7^n = 5m + 3$.

The condition (2) of § 31 becomes

$$5 \cdot 8 \cdot 9a^7\gamma - 23a^9 = 0.$$

Thus either $a = 0$ or $\gamma = 3a^2$.

But the power $m + 6$ of $\xi^5 + \gamma\xi$ requires $\gamma^7 = 0$.

The only possible form is thus $5\xi^5 + 5a\xi^3 + a^2\xi$.

35. The case $p^n = 3^n = 5m + 3$.

The condition (2) of § 31 becomes since $m \equiv 21 \pmod{27}$,

$$c_6^{m+4} \cdot 20a^3\gamma^3 + c_9^{m+4}a^9 - a^3\gamma^3 + a^9 = 0.$$

Hence $5\gamma = a^2$.

36. The case $p^n = 2^n = 5m + 3$, supposing $n > 3$. Thus $5m \equiv -3 \pmod{2^7}$ or $m \equiv 25 \pmod{128}$.

The powers $m + 2$ and $m + 4$ of $\xi^5 + a\xi^3 + \beta\xi^2 + \gamma\xi$ give

$$\gamma^2 + a^2\gamma + a\beta^2 = 0$$

$$a\gamma^4 + a^9 = 0.$$

Hence if $a = 0$, $\gamma = 0$; if $a \neq 0$, $\gamma = a^2$, $\beta = 0$.

But the power $m + 22$ of $\xi^5 + \beta\xi^2$ requires

$$c_{36}^{m+22} \cdot \beta^{36} = \beta^{36} = 0.$$

The only possible form is again $5\xi^5 + 5a\xi^3 + a^2\xi$.

* *American Journal of Mathematics*, vol. 18, p. 213.

37. The case $p^n = 2^3$.

The third and fifth powers require respectively

$$\begin{aligned}\gamma^2 + a^2\gamma + a\beta^2 &= 0 \\ \gamma + a\gamma^4 + a^4\beta &= 0,\end{aligned}$$

of which the former is the square of the latter. Hence either $a = \gamma = 0$ or $\beta = a^3\gamma + a^4\gamma^4$.

But $\xi^5 + \beta\xi^2$ vanishes for $\xi = \beta^{1/3}$, every mark in the $GF[2^3]$ being a cube by § 18.

By replacing ξ by $a^{1/2}\xi$ and γ by $a^2\gamma$, the quintic

$$\varphi(\xi) = \xi^5 + a\xi^3 + (a^3\gamma + a^4\gamma^4)\xi^2 + \gamma\xi$$

becomes

$$a^{5/2}\{\xi^5 + \xi^3 + (\gamma + \gamma^4)\xi^2 + \gamma\xi\}.$$

Hence the quintic $\varphi(\xi)$ will vanish only for $\xi = 0$ if the resultant of

$$\xi^5 + \xi^3 + (\gamma + \gamma^4)\xi^2 + \gamma\xi \text{ and } \xi^7 = 1$$

is $\neq 0$. This resultant may be written as a cyclic determinant whose first row is

$$0, 1, 0, 1, \gamma + \gamma^4, \gamma, 0.$$

On expansion it becomes

$$\gamma^7 + \gamma^6 + \gamma^5 + \gamma^4 + \gamma^3 + \gamma^2 + \gamma = (\gamma^8 - \gamma)/(\gamma - 1),$$

which is $\neq 0$ only when $\gamma = 1$.

The only suitable quintic on 8 letters is thus

$$\xi^5 + a\xi^3 + a^2\xi.$$

38. Summary of §§ 31–37. The only possible substitution quintic on $p^n = 5m + 3$ letters is reducible to the form

$$5\xi^5 + 5a\xi^3 + a^2\xi, \quad a \text{ arbitrary},$$

except for $p^n = 13$ when we have the additional form

$$5\xi^5 + 5a\xi^3 + 2a^2\xi,$$

a being a quadratic non-residue of 13.

39. Theorem. $5\xi^5 + 5a\xi^3 + a^2\xi$, where a is an arbitrary mark of the $GF[p^n]$, is suitable to represent a substitution on its p^n marks, if p is a prime number of the form $5m \pm 2$ and n is odd.

For if not we must have for two different values of ξ , say η and φ , the following equation :

$$5\eta^5 + 5a\eta^3 + a^2\eta = 5\varphi^5 + 5a\varphi^3 + a^2\varphi$$

or

$$(\eta - \varphi) \{5(\eta^4 + \eta^3\varphi + \eta^2\varphi^2 + \eta\varphi^3 + \varphi^4) + 5a(\eta^2 + \eta\varphi + \varphi^2) + a^2\} = 0.$$

Hence since $\eta \neq \varphi$,

$$5\{\eta^4 + \varphi^4 + (\eta\varphi + a)(\eta^2 + \eta\varphi + \varphi^2)\} + a^2 = 0. \quad (1)$$

(a) Suppose $p > 2$.

Making the substitution

$$\eta = \lambda + \mu, \quad \varphi = \lambda - \mu$$

$$5\{5\lambda^4 + 10\lambda^2\mu^2 + \mu^4 + 3a\lambda^2 + a\mu^2\} + a^2 = 0.$$

Multiply by 16 and substitute

$$20\lambda^2 = 4\rho - a, \quad 4\mu^2 = 4\sigma - a.$$

We thus reach the simple form

$$16(\rho^2 + 10\rho\sigma + 5\sigma^2) = 0,$$

or

$$(\rho + 5\sigma)^2 = 20\sigma^2 = 5(2\sigma)^2.$$

But* $+5$ is a quadratic residue of no odd number of the form $5m + 2$ or $5m + 3$. Hence 5 is a not-square in the $GF[p^n]$, n being odd and $p \equiv 5m + 2$.

(b) Suppose $p = 2$.

Making in (1) the substitution

$$\eta + \varphi = \lambda, \quad \eta \cdot \varphi = \mu,$$

$$\lambda^4 + a\lambda^2 + a^2 = \mu(\lambda^2 + \mu + a). \quad (2)$$

Put $\lambda^2 = \nu$ and multiply through by $\nu + \mu$:

$$\nu^3 + a\nu^2 + a^2\nu = \mu^3 + a\mu^2 + a^2\mu. \quad (3)$$

But, by § 18, ξ^3 is suitable to represent a substitution on 2^n letters, n odd, and hence is also

$$(\xi + a)^3 + a^3 = \xi^3 + a\xi^2 + a^2\xi.$$

Hence (3) has no solution in the $GF[2^n]$ except $\nu = \mu$, when by (2) we find $\nu = \mu = a$.

* Gauss, *Disquisitiones Arithmetical*, Art. 121.

Hence if (1) is satisfied, we have

$$\eta + \varphi = a^{1/2}, \quad \eta\varphi = a.$$

But this set of values for η and φ is impossible since

$$\omega^2 + a^{1/2}\omega + a = 0$$

has no root in the $GF[2^n]$, n odd, if $a \neq 0$, i. e. if $\eta \neq \varphi$. For writing $\omega = a^{1/2}\theta$, it becomes

$$\theta^2 + \theta + 1 = 0.$$

We thus need only prove that $\theta^3 - 1 = 0$ has no root other than $\theta = 1$ in the $GF[2^n]$, n odd. But if there exists a root $\neq 1$ of

$$\theta^{2^2-1} - 1 = 0$$

(and thus having the exponent 3) which is also a root of

$$\theta^{2^n-1} - 1 = 0,$$

then* must n be even.

A general theorem comprising the one here proven is given in § 54.

40. The case $p^n = 5m + 4$.

The power $m + 1$ of $\xi^5 + a\xi^3 + \beta\xi^2 + \gamma\xi$ gives $a = 0$.

The power $m + 2$ of $\xi^5 + \beta\xi^2 + \gamma\xi$ requires

$$c_2^{m+2} \cdot 2\beta\gamma = 0.$$

Hence if $p \neq 2, \neq 3$, we have $\beta\gamma = 0$.

The power $m + 3$ requires, if $p^n > 9$,

$$c_3^{m+3}\gamma^3 + c_4^{m+3}\beta^4 = 0.$$

Now $m + 3$ is divisible by p only if $p = 11$, when p^n is not of the form $5m + 4$. If $p = 2$ (and thus $n \geq 6$, we have $m \equiv 12 \pmod{64}$). Hence for every $p^n > 9$,

$$5\gamma^3 = \beta^4.$$

Thus for $p \neq 2, \neq 3$, $\beta = \gamma = 0$ and ξ^5 is the only suitable form.

41. The case $p^n = 3^n = 5m + 4$, $n > 2$.

The power $m + 4$ requires, since $m \equiv 1 \pmod{9}$,

$$c_5^{m+4} \cdot 10\beta^3\gamma^2 = \beta^3\gamma^2 = 0.$$

Hence ξ^5 is the only suitable quintic.

* Moore, l. c. § 46.

42. The case $p^n = 3^2$.

The fourth, fifth, and seventh powers of $\xi^5 + \beta\xi^2 + \gamma\xi$ require respectively,

$$\gamma(1 + \gamma^2) + \beta^4 = 0$$

$$\beta^3(1 + \gamma^2) = 0$$

$$\beta(1 + \gamma^6) = 0.$$

The solutions of these equations are

$$\beta = 0, \gamma = 0 \quad \text{and} \quad \beta = 0, \gamma^2 + 1 = 0.$$

The suitable forms are thus

$$\xi^5 \quad \text{and} \quad \xi^5 + 2^{1/2}\xi,$$

since if the latter vanished for $\xi \neq 0$, $\xi^8 = 2$. Indeed $\xi^5 + 2^{1/2}\xi$ represents the literal substitution,

$$(0)(1, 1 + 2^{1/2})(-1, -1 - 2^{1/2})(2^{1/2}, -1 + 2^{1/2})(-2^{1/2}, 1 - 2^{1/2}).$$

43. The case $p^n = 2^n = 5m + 4$.

The power $m + 11$ requires, since $m = 64l + 12$,

$$c_{17}^{m+11} \cdot 17\beta^{16}\gamma = \beta^{16}\gamma = 0.$$

Hence $\beta = \gamma = 0$ and ξ^5 is the only suitable form.

44. Summary of §§ 40-43. ξ^5 is the only reduced substitution quintic on $p^n = 5m + 4$ letters, except for $p^n = 3^2$ when we have also $\xi^5 + 2^{1/2}\xi$.

45. $\xi^6 + a\xi^4 + \beta\xi^3 + \gamma\xi^2 + \delta\xi$.

$p^n = 6m + 5$, since here p is prime to 6 and since $p^n \neq 6m + 1$.

The power $m + 1$ requires $a = 0$.

The power $m + 2$ of $\xi^6 + \beta\xi^3 + \gamma\xi^2 + \delta\xi$ requires

$$2\beta\delta + \gamma^2 = 0. \quad (1)$$

The power $m + 3$ requires, if $p^n > 11$,

$$6\gamma\delta^2 + m(2\beta^3\delta + 3\beta^2\gamma^2) = 0. \quad (2)$$

The power $m + 4$ requires, if $p^n > 17$,

$$\delta^4 + \frac{m}{5}(30\beta^2\gamma\delta^2 + 20\beta\gamma^3\delta + \gamma^5) + \frac{m(m-1)}{5 \cdot 6}(6\beta^5\delta + 15\beta^4\gamma^2) = 0. \quad (3)$$

Substituting γ^2 from (1) into (2) and (3),

$$6\gamma\delta^2 - 4m\beta^3\delta = 0 \quad (4)$$

$$\delta^4 - \frac{6m}{5}\beta^2\gamma\delta^2 - \frac{4m(m-1)}{5}\beta^5\delta = 0. \quad (5)$$

From (4) and (5)

$$\delta^4 - \frac{4m(2m-1)}{5}\beta^5\delta = 0. \quad (6)$$

Multiplying (1) by $m\beta^2$ and subtracting from (2),

$$6\gamma\delta^2 + 2m\beta^2\gamma^2 = 0.$$

If $p = 5$, $m \equiv 0 \pmod{5}$, so that $\gamma\delta^2 = 0$ and then by (6) $\delta = 0$. If $p \neq 5$, suppose $\gamma \neq 0$. Then

$$m\beta^2\gamma = -3\delta^2.$$

Substituting this in (5),

$$23\delta^4 - 4m(m-1)\beta^5\delta = 0.$$

Combining with (6),

$$(41m - 18)\delta^4 = 0 \text{ or } 313\delta^4 = 0.$$

Since 313 is a prime not of the form $6m + 5$, $\delta = 0$. Hence must $\gamma = 0$, so that $\beta\delta = 0$ and by (6) $\delta = 0$. But the power $3m + 2$ of $\xi^6 + \beta\xi^3$ gives ξ^{18m+12} and no other term with exponent divisible by $6m + 4$. Hence there is no suitable sextic when $p^n > 17$. I have shown* that $p = 17$, $n = 1$ leads to no suitable septic; while $p = 11$, $n = 1$ leads to the following substitution quantities:

$$\xi^6 \pm c^2\tilde{\xi}^3 + c\tilde{\xi}^2 \pm 5\tilde{\xi}, \quad c \text{ being a quadratic residue of } 11.$$

$$\xi^6 \pm 4c^2\tilde{\xi}^3 + c\tilde{\xi}^2 \pm 4\tilde{\xi}, \quad c = 0 \text{ or a quadratic non-residue of } 11.$$

$$\xi^6 \pm 2\tilde{\xi}.$$

A preliminary study of septics, §§ 46-50.

$$\xi^7 + a\tilde{\xi}^5 + \beta\tilde{\xi}^4 + \gamma\tilde{\xi}^3 + \delta\tilde{\xi}^2 + \varepsilon\tilde{\xi}.$$

46. The case $p^n = 7m + 6$.

The power $m + 1$ requires $a = 0$.

The power $m + 2$ requires, if $p \neq 2$,

$$7\beta\varepsilon + 7\gamma\delta - \beta^3 = 0. \quad (1)$$

* *American Journal of Mathematics*, Vol. 18, pp. 216-217.

The power $m + 3$ requires, if $p > 5$ and $p^n \neq 13$,

$$7^2(\gamma\epsilon^2 + \delta^2\epsilon) - 7(6\beta^2\gamma\epsilon + 3\beta^2\delta^2 + 6\beta\gamma^2\delta + \frac{1}{2}\gamma^4) + \frac{13}{2}\beta^4\gamma = 0. \quad (2)$$

Rejecting the special values, 2, 5, 13, etc., we may prove that if any *one* of the four coefficients $\beta, \gamma, \delta, \epsilon$ be zero, then all are zero. To handle (1), (2) and the very lengthy conditions given by the powers $m + 4$ and $m + 5$; when $\beta, \gamma, \delta, \epsilon$ are all $\neq 0$, is perhaps impracticable.

Suppose, for example, $\gamma = 0$. Then (1) and (2) become

$$\beta^3 = 7\beta\epsilon; \quad 7\delta^2\epsilon = 3\beta^2\delta^2.$$

Thus $\delta = 0$; for if not

$$7\epsilon = 3\beta^2 \text{ and thus } \beta^3 = 3\beta^3.$$

The power $m + 5$ of $\xi^7 + \beta\xi^4 + \epsilon\xi$ requires

$$7^5\epsilon^5 - 7^4 \cdot 15\beta^2\epsilon^4 + 7^3 \cdot 65\beta^4\epsilon^3 - 7^2 \cdot 130\beta^6\epsilon^2 + \frac{65 \cdot 27}{2}\beta^8\epsilon - \frac{13 \cdot 51}{14}\beta^{10} = 0.$$

If $\beta \neq 0$, $\beta^2 = 7\epsilon$ and the last equation becomes $-\beta^{10} = 0$. Thus if $\gamma = 0$, then $\beta = \delta = \epsilon = 0$, certain values of p^n being excepted.

47. The case $p^n = 7m + 5$.

The power $m + 1$ requires $\beta = 0$. If either α, γ , or ϵ be zero, we can prove that all are zero. If $\delta = 0$, the conditions given by the powers $m + 2$ and $m + 4$ (of 5 and 19 terms respectively) are satisfied by

$$7\gamma = 2a^2, \quad 7^2\epsilon = a^3.$$

48. The case $p^n = 7m + 4$.

The power $m + 1$ requires, if $p \neq 3$,

$$7\gamma = 2a^2.$$

We may prove that if $a = 0$, then $\beta = \gamma = \delta = \epsilon = 0$; that if $\beta = 0$ then $\delta = 0$ and $7^2\epsilon = a^3$.

49. The case $p^n = 7m + 3$.

The power $m + 1$ requires, if $p \neq 2$, $7\delta = 3a\beta$.

We may prove that if $a = 0$, then $\beta = \gamma = \delta = \epsilon = 0$; if $\beta = 0$ then $\delta = 0$ and the conditions given by the powers $m + 2$ and $m + 4$ (containing seven and twenty-one terms respectively) are seen to be satisfied by

$$7\gamma = 2a^2, \quad 7^2\epsilon = a^3.$$

50. The case $p^n = 7m + 2$.

The conditions are quite unwieldy even when $\alpha = 0$. If $\beta = 0$, then $\delta = 0$, $7\delta = 2\alpha^2$, $7^2\varepsilon = \alpha^3$.

Quantics with an infinite range of suitability, §§ 51-56.

51. We have found that the quintic

$$5\xi^5 + 5a\xi^3 + a^2\xi,$$

a being an arbitrary mark of the $GF[p^n]$, is suitable to represent a substitution on its p^n marks, if and only if p^n be of the form $5m \pm 2$. Also in our preliminary survey of septics, the quantic

$$7^2\xi^7 + 7^2a\xi^5 + 2 \cdot 7a^2\xi^3 + a^3\xi,$$

a being an arbitrary mark of the $GF[p^n]$, stood out in a prominent way as probably suitable on its p^n marks if and only if p^n be of the form $7m \pm 2$ or $7m \pm 3$. Note further that there is no suitable cubic other than ξ^3 . Thus is suggested the possible existence of a quantic of odd prime degree k which is suitable to represent a substitution on the marks of every $GF[p^n]$, except when p^n is of the form $km \pm 1$.

52. Suppose the reduced quantic belonging to the $GF[p^n]$,

$$\xi^k + a_2\xi^{k-2} + a_3\xi^{k-3} + a_4\xi^{k-4} + \dots + a_{k-1}\xi, \quad (1)$$

whose degree k is an odd prime number $\neq p$, is suitable to represent a substitution on the p^n marks of the field for every p^n of the form $km + 2$, $km + 3$, $km + 4$, $\dots$, or, $km + (k - 3)$. We do not at first assume it suitable on $p^n = km + (k - 2)$ letters, in which case the power $m + 1$ requires

$$(m + 1) a_3 = a_3 = 0, \text{ if } p \neq 2.$$

For $p^n = km + (k - 3)$, the power $m + 1$ requires

$$(m + 1) a_4 + \frac{(m + 1)m}{2} a_2^2 = 0,$$

or, if $p \neq 3$,

$$ka_4 = \frac{k - 3}{2} a_2^2.$$

For $p^n = km + (k - 4)$, the power $m + 1$ requires if $p \neq 2$,

$$ka_5 = (k - 4) a_2 a_3.$$

For $p^n = km + (k - 5)$, the power $(m + 1)$ requires, if $p \neq 5$,

$$k^2 a_6 - \frac{k(k - 5)}{2} (a_3^2 + 2a_2 a_4) + \frac{(k - 5)(2k - 5)}{2 \cdot 3} a_2^3 = 0,$$

or

$$k^2 a_6 = \frac{(k-4)(k-5)}{2 \cdot 3} a_2^3 + \frac{k(k-5)}{2} a_3^2.$$

For $p^n = km + (k-6)$, the power $m+1$ requires, if $p \neq 2, \neq 3$,

$$k^2 a_7 = k(k-6)(a_2 a_5 + a_3 a_4) + \frac{(k-6)(2k-6)}{2} a_2^2 a_3 = 0,$$

or

$$k^2 a_7 = \frac{(k-5)(k-6)}{2} a_2^2 a_3.$$

Similarly, for $p^n = km + (k-7)$, the power $m+1$ requires, if $p \neq 7$,

$$k^3 a_8 = \frac{(k-5)(k-6)(k-7)}{2 \cdot 3 \cdot 4} a_2^4 + \frac{k(k-6)(k-7)}{2} a_2 a_3^2;$$

for $p^n = km + (k-8)$, $p \neq 2$, the power $m+1$ requires

$$k^3 a_9 = \frac{(k-6)(k-7)(k-8)}{2 \cdot 3} a_2^3 a_3 + \frac{k(k-7)(k-8)}{2 \cdot 3} a_3^3;$$

for $p^n = km + (k-9)$, $p \neq 3$, the power $m+1$ requires

$$k^4 a_{10} = \frac{(k-6)(k-7)(k-8)(k-9)}{2 \cdot 3 \cdot 4 \cdot 5} a_2^5 + \frac{k(k-7)(k-8)(k-9)}{4} a_2^2 a_3^3.$$

It would be impracticable to attempt to calculate the general coefficient in this way. It is to be noted that if $p > k$ every coefficient is expressed uniquely in terms of a_2 and a_3 .

53. The sum s_k of the k th powers of the roots of the cubic

$$\eta^3 - \xi \eta^2 - \frac{a_2}{k} \eta - \frac{a_3}{k} = 0 \quad (2)$$

is given by Waring's formula thus :

$$s_k = \sum_{\lambda} \frac{\pi(\lambda_1 + \lambda_2 + \lambda_3 - 1)}{\pi(\lambda_1) \pi(\lambda_2) \pi(\lambda_3) \cdot k^{\lambda_2 + \lambda_3 - 1}} \cdot a_2^{\lambda_2} a_3^{\lambda_3} \xi^{\lambda_1} \quad (3)$$

where $\pi(t) = t!$ with the convention that $\pi(0) = 1$, and where the summation extends over $\lambda_1, \lambda_2, \lambda_3$ such that

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 = k.$$

Arranging according to descending powers of ξ , we have

$$\begin{aligned}
 s_k = & \xi^k + a_2 \xi^{k-2} + a_3 \xi^{k-3} + \frac{k-3}{2k} a_2^2 \xi^{k-4} + \frac{k-4}{k} a_2 a_3 \xi^{k-5} \\
 & + \left\{ \frac{(k-4)(k-5)}{6k^2} a_2^3 + \frac{k-5}{2k} a_3^2 \right\} \xi^{k-6} + \frac{(k-5)(k-6)}{2k^2} a_2^2 a_3 \xi^{k-7} \\
 & + \left\{ \frac{(k-5)(k-6)(k-7)}{24k^3} a_2^4 + \frac{(k-6)(k-7)}{2k^2} a_2 a_3^2 \right\} \xi^{k-8} \\
 & + \left\{ \frac{(k-6)(k-7)(k-8)}{6k^3} a_2^3 a_3 + \frac{(k-7)(k-8)}{6k^2} a_3^3 \right\} \xi^{k-9} \\
 & + \left\{ \frac{(k-6)(k-7)(k-8)(k-9)}{5! k^4} a_2^5 + \frac{(k-7)(k-8)(k-9)}{4k^3} a_2^2 a_3^2 \right\} \xi^{k-10} + \dots \quad (4)
 \end{aligned}$$

Thus the first ten coefficients in s_k are exactly the corresponding coefficients of the quantic (1) as calculated in § 52. A complete identification of s_k with (1) will be carried out for the most interest case, viz, when $a_3 = 0$, which happens when the range of suitability of (1) excludes only the combinations $p^n = km \pm 1$. For then by § 54 the quantic $s_k(\xi)$ will satisfy the conditions derived by the method of § 52 which have an unique solution in terms of a_2 .

For $a_3 = 0$, (3) reduces to

$$s_k = \sum_{l=0}^{(k-1)/2} \frac{\pi(k-l-1)}{\pi(l)\pi(k-2l)} a_2^{l/k^{l-1}} \xi^{k-2l}.$$

Thus

$$\eta_1^k + \eta_2^k = \xi^k + k \cdot \sum_{l=1}^{(k-1)/2} \frac{(k-l-1)(k-l-2)\dots(k-2l+1)}{2 \cdot 3 \dots l} \left[\frac{a_2}{k} \right]^l \xi^{k-2l}, \quad (5)$$

where η_1 and η_2 are the roots of the quadratic

$$\eta^2 - \xi\eta - \frac{a^2}{k} = 0. \quad (6)$$

54. Theorem. *The quantic*

$$\theta_k(\xi, a) = \xi^k + k \sum_{l=1}^{(k-1)/2} \frac{(k-l-1)\dots(k-2l+1)}{2 \cdot 3 \dots l} a^l \xi^{k-2l},$$

where k is any odd integer* not divisible by p , and a any mark except† zero of the $GH[p^n]$, is suitable to represent a substitution on its p^n marks, if and only if p^{2n-1} be relatively prime to k .

* k is not necessarily prime. The proof in § 52 that $\theta_k(\xi, a)$ is the *only* quantic with the range of suitability $p^n = km + 2, + 3, \dots + (k-2)$ requires that k be a prime number.

† See § 18.

We are to prove that under the named restrictions

$$\theta_k(\xi, a) = \beta \quad (7)$$

has a solution ξ in the $GF[p^n]$, β being an arbitrary mark of that field.

Now by the transformation

$$\xi = \eta - \frac{a}{\eta} \quad (6')$$

the quantic is given the form

$$\eta^k - \left[\frac{a}{\eta} \right]^k. \quad (5')$$

Thus equation (7) becomes

$$\eta^{2k} - \beta \eta^k - a^k = 0. \quad (7')$$

Substituting $Y = \eta^k$, this becomes

$$Y^2 - \beta Y + (-a)^k = 0,$$

which *belongs* to the $GF[p^n]$ and is for *every* β resolvable in the $GF[p^{2n}]$ but not in the $GF[p^n]$. Call its roots Y and $\bar{Y}$.

Now the equation

$$\eta^k = Y$$

is solvable in the $GF[p^{2n}]$, Y being an arbitrary mark of that field, if and only if $p^{2n} - 1$ be relatively prime to k .

Then if η be a mark of the $GF[p^{2n}]$ satisfying (7'), we must prove that

$$\xi = \eta - \frac{a}{\eta}$$

falls into the lower field $GF[p^n]$. Since Y and $\bar{Y}$ are conjugate marks with respect to the $GF[p^n]$ whose product is $(-a)^k$, we have

$$\eta \bar{\eta} = -a.$$

Hence

$$\xi = \eta - a/\eta = \eta + \bar{\eta} = \bar{\xi}$$

so that indeed* ξ belongs to the $GF[p^n]$.

55. The *algebraic* roots of (7) are

$$\rho \varepsilon^m + \sigma \varepsilon^{k-m} \quad (m = 0, 1, \dots, k-1)$$

where

$$\rho, \sigma = \sqrt[k]{\beta/2 \pm \sqrt{\beta^2/4 + a^k}}$$

* Moore, l. c. § 51.

and ϵ is a primitive k th root of unity. This is a straight generalization of Cardan's formula for the roots of the cubic and also of Vallès' solution of the quintic*

$$x^5 - ax^3 + \frac{a^2}{5}x - \beta = 0.$$

It is evident that the algebraic solution of (7) for a and β arbitrary is equivalent to the extraction of the k th root of an arbitrary complex quantity and hence equivalent to the partitioning of an arbitrary angle into k equal parts.

56. The study of the quantic $\varphi_k(\xi, a_2, a_3)$ derived as in § 52, or conjecturally (when $a_3 \neq 0$) as in § 53, is made here only for the case $a_3 = 0$. It is to be expected that, for $a_3 \neq 0$, it is a substitution quantic at least for certain special values of k, p, n, a_2 and a_3 . Thus if $k = 5, p = 7$, we find

$$\xi^5 - a_2 \xi^2 - a_3 \xi^2 = 3a_2^2 \xi$$

which by § 30 includes the three types of quintics suitable on 7 letters, as well as the one suitable on 7^n letters, n being odd.

SECTION III.—Degree a Power of p .

Quantics with all exponents powers of p , §§ 57–59.

57. Theorem.† The reduced quantic

$$\chi(X) = \sum_{i=1}^n A_i X^{p^{n(i-1)}},$$

belonging to the $GF[p^{nm}]$, will represent a substitution on its p^{nm} marks if and only if

$$\chi(X) = 0 \tag{1}$$

has no root in the $GF[p^{nm}]$ other than $X = 0$.

For it will be a substitution quantic if and only if it be impossible to find two different marks X_1 and X_2 of the $GF[p^{nm}]$ such that

$$\chi(X_1) = \chi(X_2)$$

or

$$\chi(X_1 - X_2) = 0.$$

Corollary. $X^{p^{nr}} - AX^{p^{ns}}$ represents a substitution on p^{nm} letters if and only if $A = 0$ or A is a not $(p^{nr} - p^{ns})$ power in the $GF[p^{nm}]$.

* M. F. Vallès, *Formes imaginaires en Algèbre*, Vol. I, pp. 90–92, 1869.

† I reached this result independently. Cf. Mathieu, l. c. Vol. 6, 1861, p. 275; also Betti, l. c. Vol. 3, p. 74, 1852. For the connection with linear substitutions see Part II, Section III.

Dividing out X from (4) we obtain for $k = 0, 1, 2, \dots, m-1$ a system of m equations equivalent to the system (1) and (2), since from the former we can pass back to the latter.

59. Owing to the objection that may be made against the usual proof of Sylvester's dialytic method of elimination, the following proof that (3) is the resultant of (1) and (2) is given.

Lemma.* The necessary and sufficient condition that m marks $\mathcal{Q}_0, \mathcal{Q}_1, \dots, \mathcal{Q}_{m-1}$ of the $GF[p^{nm}]$ shall be linearly independent with respect to the $GF[p^n]$ is that the determinant

$$\begin{vmatrix} \mathcal{Q}_0 & \mathcal{Q}_1 & \dots & \mathcal{Q}_{m-1} \\ \mathcal{Q}_0^{p^n} & \mathcal{Q}_1^{p^n} & \dots & \mathcal{Q}_{m-1}^{p^n} \\ \mathcal{Q}_0^{p^{2n}} & \mathcal{Q}_1^{p^{2n}} & \dots & \mathcal{Q}_{m-1}^{p^{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{Q}_0^{p^{n(m-1)}} & \mathcal{Q}_1^{p^{n(m-1)}} & \dots & \mathcal{Q}_{m-1}^{p^{n(m-1)}} \end{vmatrix} \neq 0 \quad (\mathcal{Q}_j^{p^{ni}} |, (j^i = 0, 1, \dots, m-1)) \quad (5)$$

shall $\neq 0$.

It is sufficient; for if $\mathcal{Q}_0, \mathcal{Q}_1, \dots, \mathcal{Q}_{m-1}$ be linearly dependent in the $GF[p^n]$, i. e. if a relation

$$\sum_{i=0}^{m-1} \gamma_i \mathcal{Q}_i = 0 \quad (6)$$

holds where $\gamma_0, \gamma_1, \dots, \gamma_{m-1}$ are marks of the $GF[p^n]$ not all zero, then will the determinant (5) vanish.

It is necessary; for if (5) be zero, write

$$\mathcal{Q}_i = \sum_{j=0}^{m-1} \mu_{ij} R^j \quad (i = 0, 1, \dots, m-1)$$

where R is a primitive root of the $GF[p^{nm}]$ and the μ_{ij} 's are marks of the $GF[p^n]$. Then

$$\mathcal{Q}_j^{p^{ni}} = \mu_{ij} \cdot (R^j)^{p^{ni}}, \quad (i, j = 0, 1, \dots, m-1)$$

* A more general theorem is given by E. H. Moore. *A two-fold generalization of Fermat's theorem*, *Bulletin of the American Mathematical Society*, second series, Vol. 2, April, 1896.

where, writing in full the determinant in R , we have*

$$\begin{vmatrix} 1 & , & 1 & , & \dots & , & 1 \\ R & , & R^{p^n} & , & \dots & , & R^{p^{n(m-1)}} \\ R^2 & , & R^{2p^n} & , & \dots & , & R^{2p^{n(m-1)}} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ R^{m-1} & , & R^{(m-1)p^n} & , & \dots & , & R^{(m-1)p^{n(m-1)}} \end{vmatrix} = H(R^{p^{ns}} - R^{p^{nt}}) \quad (7)$$

$s, t = 0, 1, \dots, m-1$
 $s > t$

which $\neq 0$, R being a primitive root in the $GF[p^{nm}]$. Hence $\mu_{ij} = 0$, so that a linear relation (6) exists, in which not every γ_i is zero, or $\mathcal{Q}_0, \mathcal{Q}_1, \dots, \mathcal{Q}_{m-1}$ are linearly dependent in the $GF[p^n]$.

The condition on $A_1, A_2, \dots, A_m$ that

$$X' = \sum_{i=1}^m A_i X^{p^{n(m-i)}} \quad (8)$$

shall represent a substitution on p^{nm} letters is the same as the condition under which $X'_1, X'_2, \dots, X'_m$ shall be linearly independent with respect to the $GF[p^n]$, when it is given that $X_1, X_2, \dots, X_m$ are similarly independent. By our lemma, the latter condition is

$$X_j'^{p^{ni}} \neq 0. \quad (i, j = 0, 1, \dots, m-1)$$

Applying (8) this determinant becomes

$$\begin{vmatrix} A_1 X_1^{p^{n(m-1)}} + A_2 X_1^{p^{n(m-2)}} + \dots + A_m X_1 & , & \dots & , & A_1 X_m^{p^{n(m-1)}} + \dots + A_m X_m \\ A_1^{p^n} X_1 & + A_2^{p^n} X_1^{p^{n(m-1)}} + \dots + A_m^{p^n} X_1^{p^n} & , & \dots & , & A_1^{p^n} X_m & + \dots + A_m^{p^n} X_m^{p^n} \\ A_1^{p^{2n}} X_1^{p^n} & + A_2^{p^{2n}} X_1^{p^{2n}} & + \dots + A_m^{p^{2n}} X_1^{p^{2n}} & , & \dots & , & A_1^{p^{2n}} X_m^{p^n} & + \dots + A_m^{p^{2n}} X_m^{p^{2n}} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{vmatrix}$$

which equals the product of determinant (3) of § 58 by

$$\begin{vmatrix} X_1^{p^{n(m-1)}} & , & X_2^{p^{n(m-1)}} & , & \dots & , & X_m^{p^{n(m-1)}} \\ X_1^{p^{n(m-2)}} & , & X_2^{p^{n(m-2)}} & , & \dots & , & X_m^{p^{n(m-2)}} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ X_1 & , & X_2 & , & \dots & , & X_m \end{vmatrix}$$

* Baltzer, *Determinanten*, p. 85.

But by (5) this $\neq 0$, $X_1, \dots, X_m$ being supposed linearly independent in the $GF[p^n]$.

General theorems on $SQ[p^r; p^n]$, §§ 60–68.

60. In studying the quantic belonging to the $GF[p^n]$,

$$\tilde{\zeta}^{p^r} + a_k \tilde{\zeta}^{p^r-k} + a_{k+1} \tilde{\zeta}^{p^r-k-1} + \dots + a_{p^r-1} \tilde{\zeta},$$

in which $a_k \neq 0$, and $k < p^r - 1$ it is found desirable to compute the power

$$p^{n-r} + k(p^{n-2r} + p^{n-3r} + \dots + p^{r+t}) + h,$$

where t is the least positive residue of n modulo r and $h < p^{r+t}$.

Let the general term of the expansion be

$$(\tilde{\zeta}^{p^r})^{a_0} \cdot (a_k \tilde{\zeta}^{p^r-k})^{a_k} \cdot (a_{k+1} \tilde{\zeta}^{p^r-k-1})^{a_{k+1}} \dots (a_{p^r-1} \tilde{\zeta})^{a_{p^r-1}},$$

where we thus have

$$a_0 + a_k + a_{k+1} + \dots + a_{p^r-1} = p^{n-r} + k p^{n-2r} + \dots + h, \quad (1)$$

$$s = p^r a_0 + (p^r - k) a_k + (p^r - k - 1) a_{k+1} + \dots + a_{p^r-1} = p^n - 1. \quad (2)$$

I shall use the abbreviations

$$s_1 = p^r a_0 + (p^r - k) a_k + a_{k+1} + a_{k+2} + \dots + a_{p^r-1};$$

$$s_2 = p^r a_0 + (p^r - k) a_k + (p^r - k - 1)(a_{k+1} + a_{k+2} + \dots + a_{p^r-1}).$$

61. By equation (2)

$$a_0 = (p^n - 1)/p^r < p^{n-r}.$$

Hence by an application of § 14 to (1),

$$a_0 \leq k p^{n-2r} + k \cdot p^{n-3r} + \dots + k \cdot p^{r+t} + h.$$

Suppose at first

$$a_0 = k \cdot p^{n-2r} + k \cdot p^{n-3r} + \dots + h - x,$$

where

$$0 = x \leq k p^{n-3r} + k p^{n-4r} + \dots + h.$$

Then by (1)

$$a_k + a_{k+1} + \dots + a_{p^r-1} = p^{n-r} + x.$$

If $a_k = p^{n-r} + y$, where $0 \leq y \leq x$, we readily find

$$s_1 = p^n + k p^{n-2r} + k p^{n-3r} + \dots + h p^r - (p^r - 1)x + (p^r - k - 1)y.$$

$$\geq p^n + k p^{n-2r} + \dots + h p^r - p^r x > p^n - 1.$$

Hence $s \geq s_1 > p^n - 1$, contrary to (2).

If $a_k = y$, then

$$s_2 = (p^r - 1)p^{n-r} + k \cdot p^{n-2r} + kp^{n-3r} + \dots + hp^r - (k+1)x + y.$$

Hence $s \geq s_2 < p^n - 1$.

Applying § 14, we conclude that $a_0 < kp^{n-2r}$ and thus

$$a_0 \leq (k-1)p^{n-2r} + kp^{n-3r} + \dots + k \cdot p^{r+t} + h.$$

62. We may prove by induction the theorem

$$a_0 \leq (k-1)(p^{n-2r} + p^{n-3r} + \dots + p^{r+t}) + h.$$

Thus, to make the general step, suppose

$$\begin{aligned} a_0 &= (k-1)(p^{n-2r} + p^{n-3r} + \dots + p^{n-mr}) \\ &\quad + k(p^{n-(m+1)r} + p^{n-(m+2)r} + \dots + p^{r+t}) + h - x', \end{aligned}$$

where

$$0 \leq x' \leq k(p^{n-(m+2)r} + p^{n-(m+3)r} + \dots + p^{r+t}) + h.$$

Then

$$a_k + a_{k+1} + \dots + a_{p^r-1} = p^{n-r} + p^{n-2r} + \dots + p^{n-mr} + x'.$$

If $a_k = p^{n-r} + p^{n-2r} + \dots + p^{n-mr} + y'$, $0 \leq y' \leq x'$, then

$$s_1 = p^n + k(p^{n-(m+1)r} + \dots + p^{2r+t}) + hp^r - (p^r - 1)x' + (p^r - k - 1)y'.$$

Hence $s \geq s_1 > p^n - 1$.

If $a_k = p^{n-r} + p^{n-2r} + \dots + p^{n-(m-1)r} + y'$,

$$s_2 = p^n - p^{n-mr} + k(p^{n-(m+1)r} + \dots + p^{2r+t}) + hp^r - (k+1)x' + y'.$$

Hence $s \geq s_2 < p^n - 1$.

If a_k have a value less than that last supposed, much more will s be $< p^n - 1$. Hence

$$a_0 < (k-1)(p^{n-2r} + p^{n-3r} + \dots + p^{n-mr}) + kp^{n-(m+1)r}.$$

Hence finally,

$$a_0 \leq (k-1)(p^{n-2r} + \dots + p^{n-(m+1)r}) + k(p^{n-(m+2)r} + \dots + p^{r+t}) + h.$$

63. Let g denote a positive integer and write

$$a_0 = (k-1)(p^{n-2r} + p^{n-3r} + \dots + p^{r+t}) + h - g. \quad (3)$$

Here g is not a multiple of p , since then would also $a_k + a_{k+1} + \dots + a_{p^r-1}$ and by § 14 s would likewise be a multiple of p .

From (1), (2) and (3) we readily find

$$a_k + a_{k+1} + \dots + a_{p^r-1} = p^{n-r} + p^{n-2r} + \dots + p^{r+t} + g \quad (4)$$

$$\begin{aligned} (p^r - k) a_k + (p^r - k - 1) a_{k+1} + \dots + a_{p^r-1} &= p^n - 1 - p^r a_0 \\ &= (p^r - k) (p^{n-r} + p^{n-2r} + \dots + p^{r+t}) + p^r (kp^t + g - h) - 1. \end{aligned} \quad (5)$$

Multiplying (4) by $p^r - k$ and subtracting (5),

$$a_{k+1} + 2a_{k+2} + 3a_{k+3} + \dots + (p^r - k - 1) a_{p^r-1} = p^r (h - kp^t) - kg + 1. \quad (6)$$

Thus

$$\begin{aligned} g &\leq \{ p^r (h - kp^t) + 1 \} / k \\ h &> kp^t, \text{ unless } h = k = 1, t = 0. \end{aligned} \quad (7)$$

The calculation of the condition given by the power

$$p^{n-r} + k (p^{n-2r} + p^{n-3r} + \dots + p^{r+t}) + h$$

consists in taking for g in turn each of the values*

$$1, 2, 3, \dots, E \left[\frac{p^r (h - kp^t) + 1}{k} \right],$$

and determining by (6) every possible set of values for $a_{k+1}, a_{k+2}, \dots, a_{p^r-1}$ which form a partition of

$$p^{n-r} + p^{n-2r} + \dots + p^{r+t} + g$$

of the kind required by § 14. Then (4) gives the a_k and finally (3) the a_0 corresponding to each set.

64. The value $g = 1$ may be discarded if

$$kp^t < h \leq (k+1)p^t,$$

provided $k > 1$ when the equality sign holds.

For by (5),

$$a_k < p^{n-r} + p^{n-2r} + \dots + p^{r+t};$$

and hence by (4),

$$a_k \leq p^{n-r} + p^{n-2r} + \dots + p^{r+t} + 1.$$

Then

$$s_2 \leq (p^r - 1) (p^{n-r} + p^{n-2r} + \dots + p^{r+t}) + hp^r - k + p^{r+t} (p^r - k - 1).$$

Hence

$$s \leq s_2 \leq p^n + hp^r - (k+1)p^{r+t} - k < p^{n-1}$$

if

$$h < (k+1)p^t \text{ or } h = (k+1)p^t, k > 1.$$

* $E(x)$ denotes the greatest integer in x .

65. Theorem. If $t = 0$, i. e. n be a multiple of r , the coefficient $a_1 = 0$.

For $p^r = 2$, $\xi^2 + a_1\xi$ is suitable on 2^n letters (by § 57) if and only if it vanishes only when $\xi = 0$ i. e. if $a_1 = 0$.

For $p^r > 2$, consider the power

$$p^{n-r} + p^{n-2r} + \dots + p^r + 1.$$

Making $h = k = 1$, $t = 0$, we have $g = 1$ and hence

$$a_0 = 0, a_1 = p^{n-r} + \dots + p^r + 1, a_2 = a_3 = \dots = a_{p^r-1} = 0.$$

The condition is thus

$$a_1 p^{p^r-r} + \dots + p^{r+1} = 0.$$

66. Theorem. If the quantic belonging to the $GF[p^n]$, $p > 2$,

$$\xi^{p^r} + a_{p^r+1} \xi^{(p^r-1)/2} + a_{(p^r+3)/2} \xi^{(p^r-3)/2} + \dots + a_{p^r-1} \xi$$

be suitable on p^n letters, then $a_{(p^r+1)/2} = 0$.

Consider the power

$$p^{n-r} + p^r + \frac{1}{2} (p^{n-2r} + p^{n-3r} + \dots + p^{r+t} + p^t) + 1.$$

Thus

$$k = (p^r + 1)/2, h = \frac{p^r + 1}{2} \cdot p^t + 1, g = 2.$$

Hence by (6) and (4)

$$a_{k+1} = a_{k+2} = \dots = a_{p^r-1} = 0, a_k = p^{n-r} + p^{n-2r} + \dots + p^{r+t} + 2.$$

The condition is thus $a_k^{a_k} = 0$.

67. Less frequently will be studied the power

$$q \cdot p^{n-r} + k (p^{n-2r} + p^{n-3r} + \dots + p^{r+t}) + h,$$

where q and k are $< p^r$ and $h < p^{r+t}$.

Similarly as in §§ 61 and 62 we may prove that

$$a_0 = (q-1)p^{n-r} + (k-1)(p^{n-2r} + \dots + p^{r+t}) + h.$$

Taking $s = q(p^n - 1)$, we find as in § 63,

$$a_0 = (q-1)p^{n-r} + (k-1)(p^{n-2r} + \dots + p^{r+t}) + h - g$$

$$a_{k+2} + 2a_{k+3} + 3a_{k+4} + \dots + (p^r - k - 1)a_{p^r-1} = p^r(h - kp^t) - kg + q,$$

where $g > 0$, $g \not\equiv 0 \pmod{p}$.

The parts of the condition given by

$$s = q_1 (p^n - 1), \quad q_1 < q$$

can not be satisfactorily obtained by a similar analysis. See the direct method used in § 73 (*f*).

68. Exactly as in §§ 61-63, we may prove that for the

$$p^{n-r} + k(p^{n-2r} + p^{n-3r} + \dots + p^{2r+t}) + (k+1)p^{r+t} + h$$

power of the quantic (in which the term $a_{k+1}\hat{\xi}^{p^r-k-1}$ is absent)

$$\hat{\xi}^{p^r} + a_k \hat{\xi}^{p^r-k} + a_{k+2} \hat{\xi}^{p^r-k-2} + \dots + a_{p^r-1} \hat{\xi},$$

$$a_0 = (k-1)(p^{n-2r} + \dots + p^{2r+t}) + kp^{r+t} + h - g, \quad g \geq 1;$$

$$a_k + a_{k+2} + a_{k+3} + \dots + a_{p^r-1} = p^{n-r} + p^{n-2r} + \dots + p^{r+t} + g;$$

$$2a_{k+2} + 3a_{k+3} + \dots + (p^r - k - 1)a_{p^r-1} = p^{2r+t} + hp^r - kp^{r+t} - kg + 1.$$

Determination of all reduced $SQ[p^r; p^n]$ for $p^r \geq 7$ and partially for $p^r = 11$, §§ 69-74.

69. $p^r = 2$.

By § 65 we need only consider $\hat{\xi}^2$, which is suitable on 2^n letters by § 18.

70. $p^r = 3$.

By § 65 the form is $\hat{\xi}^3 + a_2 \hat{\xi}$, which is suitable on 3^n letters by § 57, corollary, if and only if $a_2 = 0$, or $-a_2$ is a not-square in the $GF[3^n]$.

71. $p^r = 2^2$. $\hat{\xi}^4 + a_1 \hat{\xi}^3 + a_2 \hat{\xi}^2 + a_3 \hat{\xi}$ on 2^n letters.

If n be even, $a_1 = 0$ by § 65.

If n be odd, then also $a_1 = 0$. For if not we may remove the term $\hat{\xi}^2$ by a linear transformation. Consider then the power $2^{n-2} + 2^{n-4} + \dots + 2^3 + 3$ of

$$\hat{\xi}^4 + a_1 \hat{\xi}^3 + a_3 \hat{\xi}.$$

Since $a_0 \geq 0$, it follows from (3) of § 63 that $g \geq 3$; also that $g \neq 2$. By § 64, $g > 1$. The remaining value $g = 3$ gives in equation (6) of § 63,

$$2a_3 = 2^2 - 3 + 1, \text{ or } a_3 = 1.$$

Then by (4)

$$a_1 = 2^{n-2} + 2^{n-4} + \dots + 2^3 + 2.$$

The condition is thus

$$a_1^{2^{n-2} + \dots + 2^3 + 2} a_3 = 0.$$

Hence would $a_3 = 0$. But $\hat{\xi}^4 + a_1 \hat{\xi}^3$ vanishes for $\hat{\xi} = a_1$. Hence $a_1 \neq 0$ leads to no substitution quantic.

Our quantic thus becomes

$$\xi^4 + a_2 \xi^2 + a_3 \xi$$

which is suitable on 2^n letters if and only if a determinant of the form (3) in § 58 is $\neq 0$.

72. $p^r = 5$.

Cases depending on which is the first coefficient $\neq 0$.

(a) ξ^5 .

Suitable on 5^n letters by § 18.

(b) $\xi^5 + a_4 \xi$, $a_4 \neq 0$.

Suitable by corollary to § 57 if $-a_4$ is a not fourth power in the $GF[5^n]$.

(c) $\xi^5 + a_3 \xi^2 + a_4 \xi$, $a_3 \neq 0$.

Rejected by § 66.

(d) $\xi^5 + a_2 \xi^3 + a_4 \xi$, $a_2 \neq 0$.

The coefficient of ξ^2 has been removed by a linear transformation. The lowest power giving a condition is

$$5^{n-1} + 2 \cdot 5^{n-2} + 2 \cdot 5^{n-3} + \dots + 2 \cdot 5 + 3.$$

Thus $g = 2$ or $3 - E\left[\frac{5+1}{2}\right]$, since $g > 1$ by § 64.

For $g = 2$, $a_4 = 1$, $a_2 = 5^{n-1} + 5^{n-2} + \dots + 5 + 1$;

for $g = 3$, $a_4 = 0$, $a_2 = 5^{n+1} + 5^{n-2} + \dots + 5 + 3$.

The condition is thus (using § 15)

$$2^{n-2} \cdot 3! a_2^{5^{n-1} + \dots + 5 + 1} a_4 + 2^{n-2} a_2^{5^{n-1} + \dots + 5 + 3} = 0$$

or

$$a_4 = 4a_2^2.$$

The quintic is thus $\xi(\xi^2 - 2a_2)^2$, which is indeed suitable on the 5^n marks of the $GF[5^n]$, if $2a_2$ be a not-square in the field. For if, when $\gamma \neq \varphi$,

$$\gamma(\gamma^2 - 2a_2)^2 = \varphi(\varphi^2 - 2a_2)^2$$

on dividing out $\gamma - \varphi$,

$$(\gamma - \varphi)^4 + a_2(\gamma^2 + \gamma\varphi + \varphi^2) + 4a_2^2 = 0.$$

Substituting

$$\gamma = \lambda - \mu, \quad \varphi = \lambda + \mu,$$

$$(\mu^2 - 2a_2)^2 = 2a_2\lambda^2.$$

(e) The case $a_1 \neq 0$ is rejected by § 65.

73. $p^r = 7$.

(a) ξ^7 is suitable on 7^n letters.

(b) $\xi^7 + a_6 \xi$.

Suitable if $-a_6$ is a not-sixth power in the $GF[7^n]$.

(c) $\xi^7 + a_5 \xi^2, a_5 \neq 0$.

Consider the power

$$a_0 + a_5 = 2 \cdot 7^{n-1} + 4(7^{n-2} + 7^{n-3} + \dots + 7) + 5.$$

If $7a_0 + 2a_5 = 2(7^n - 1)$, then we find

$$a_5 = 6 \cdot 7^{n-2} + 3 \cdot 7^{n-3} + \dots$$

contrary to the method of partition required by § 14.

If $7a_0 + 2a_5 = 7^n - 1$, we find

$$a_0 = 2 \cdot 7^{n-2} + 2 \cdot 7^{n-3} + \dots + 2 \cdot 7 + 2; a_5 = 2 \cdot 7^{n-1} + 2 \cdot 7^{n-2} + \dots + 2 \cdot 7 + 3.$$

Hence $a_5 = 0$.

(d) $\xi^7 + a_4 \xi^3 + a_3 \xi^2 + a_6 \xi$.

Rejected by § 66.

(e) $\xi^7 + a_3 \xi^4 + a_5 \xi^2 + a_6 \xi, a_3 \neq 0$.

For the power $7^{n-1} + 3(7^{n-2} + 7^{n-3} + \dots + 7) + 4, g = 2$ giving

$$a_3^{7^{n-1} + \dots + 7 + 1} a_5 = 0, \text{ or } a_5 = 0.$$

For the power $7^{n-1} + 3(7^{n-2} + \dots + 7) + 5, g = 3, 4, \text{ or } 5$, giving

$$(3!)^{n-2} \cdot 5! \left\{ \frac{a_3^{7^{n-1} + \dots + 7 + 1} a_6^2}{2^n} + \frac{a_3^{7^{n-1} + \dots + 7 + 3} a_6}{2^{n-2} \cdot 3!} + \frac{a_3^{7^{n-1} + \dots + 7 + 5}}{2^{n-2} \cdot 5!} \right\} = 0,$$

or

$$a_3^{7^{n-1} + \dots + 7 + 1} (a_6 - 2a_3^2)^2 = 0.$$

The only possible form is thus

$$\xi (\xi^3 - 3a_3)^2.$$

(f) $\xi^7 + a_2 \xi^5 + a_4 \xi^3 + a_5 \xi^2 + a_6 \xi, a_2 \neq 0$.

The power $7^{n-1} + 2 \cdot 7^{n-2} + 2 \cdot 7^{n-3} + \dots + 2 \cdot 7 + 3$ requires

$$2^{n-2} \cdot 3! \left\{ \frac{1}{2} a_2^{7^{n-1} + \dots + 7 + 2} a_4 + \frac{1}{2} a_2^{7^{n-1} + \dots + 7} a_4^2 + a_2^{7^{n-1} + \dots + 7 + 1} a_6 \right\} = 0$$

or

$$a_2^2 a_4 + a_4^2 + 2a_2 a_6 = 0. \quad (1)$$

The power $7^{n-1} + 2 \cdot 7^{n-2} + 2 \cdot 7^{n-3} + \dots + 2 \cdot 7 + 4$ requires

$$2^{n-2} \cdot 4! a_2^{7^{n-1} + \dots + 7} a_5 \left\{ \frac{1}{6} a_5^2 + a_4 a_6 + \frac{1}{2} a_2 a_4^2 + \frac{1}{2} a_2^2 a_6 \right\} = 0.$$

(Thus $g < 7 = E \left[\frac{2 \cdot 7 + 1}{2} \right]$; so that by the partition requirements we have from (4) § 63 that $g \leq h$ or 4.)

Applying (1), either $a_5 = 0$ or else

$$a_2^2 a_5^2 = -a_2 a_4 (3a_2^2 + 5a_4)^2 \quad (2)$$

and thus $-a_2 a_4$ would be a square in the $GF[7^n]$.

Consider the power $2 \cdot 7^{n-1} + 2 \cdot 7^{n-2} + \dots + 2 \cdot 7 + 2$.

For $s = 2(7^n - 1)$, we apply § 67 for $q = h = k = 2, t = 0$. Hence

$$g = 1, a_4 = a_5 = a_6 = 0, a_0 = a_2 = 7^{n-1} + 7^{n-2} + \dots + 7 + 1.$$

The coefficient of $2(7^n - 1)$ is thus $2^n a_2^{7^{n-1} + \dots + 7 + 1}$.

For $s = 7^n - 1$, we have

$$a_0 + a_2 + a_4 + a_5 + a_6 = 2(7^{n-1} + \dots + 7 + 1)$$

$$7a_0 + 5a_2 + 3a_4 + 2a_5 + a_6 = 6(7^{n-1} + \dots + 7 + 1) = 7^n - 1.$$

Hence

$$4a_0 + 2a_2 - a_5 - 2a_6 = 0.$$

Using the notation

$$a_i = \sum_{j=0}^{n-1} c_j^{(i)} \cdot 7^j \quad (i = 0, 2, 4, 5, 6)$$

we know by § 14 that each $c_j^{(i)}$ is 0, 1, or 2 such that

$$c_j^{(0)} + c_j^{(2)} + c_j^{(4)} + c_j^{(5)} + c_j^{(6)} = 2 \quad (j = 0, 1, \dots, n-1)$$

We have immediately

$$4c_0^{(0)} + 2c_0^{(2)} - c_0^{(5)} - 2c_0^{(6)} = 7m$$

m being an integer. But m must be zero. By induction,

$$4c_j^{(0)} + 2c_j^{(2)} - c_j^{(5)} - 2c_j^{(6)} = 0 \quad (j = 0, 1, \dots, n-1)$$

Then $c_j^{(5)} = 0$ or 2. But if $c_j^{(5)} = 2$, $c_j^{(0)} = c_j^{(2)} = c_j^{(6)} = 0$ and the last equation is not satisfied. Finally, $c_j^{(0)} = 0$. Hence $a_0 = a_5 = 0$ and $a_2 = a_6$. Then

$$2a_2 = a_4 = 2(7^{n-1} + \dots + 7 + 1)$$

from which it follows that a_2 takes exactly the 2ⁿ values

$$\sum_{j=0}^{n-1} c_j^{(2)} \cdot 7^j$$

where $c_j^{(2)} = 0$ or 1. We thus obtain 2^n terms,

$$(a_2 \tilde{a}_5)^{a_2} (a_4 \tilde{a}_5)^{a_4} (a_6 \tilde{a}_5)^{a_2}$$

or

$$(a_2 a_6)^{a_2} (a_4)^{7^{n-1} + 7^{n-2} + \dots + 7 + 1 - a_2}.$$

Hence, as far as their literal parts, these 2^n terms are identical with those given by the expansion

$$(2a_2 a_6 + a_4^2)^{7^{n-1} + 7^{n-2} + \dots + 7 + 1}.$$

In order that the numerical coefficients be congruent modulo 7, we must have by § 15,

$$2^{a_2} = 2^n / \prod_{j=1}^{n-1} (c_j^{(4)}!)$$

But if l of the $c_j^{(2)}$'s are $= 1$, l of the $c_j^{(4)}$'s are zero and hence $n - l$ are $= 2$. Hence

$$\prod_{j=1}^{n-1} (c_j^{(4)}!) = 2^{n-l}.$$

$$2^{a_2} = \prod_{j=1}^{n-1} (2^{7^j c_j^{(2)}}) = \prod_{j=1}^{n-1} (2)^{c_j^{(2)}} = 2^l.$$

The identification is thus complete.

The complete condition given by the above power is thus

$$2^n a_2^{7^{n-1} + \dots + 7 + 1} + (2a_2 a_6 + a_4^2)^{7^{n-1} + \dots + 7 + 1} = 0.$$

Applying (1) and remembering that $a_2 \neq 0$,

$$(-a_2 a_4)^{(7^n - 1)/6} = -2^n. \quad (3)$$

Hence

$$(-a_2 a_4)^{(7^n - 1)/6} = (2^3)^n = 1,$$

so that $-a_2 a_4$ is a not-square in the $GF[7^n]$. Hence by (2) $a_5 = 0$.

The power $7^{n-1} + 2 \cdot 7^{n-2} + 2 \cdot 7^{n-3} + \dots + 2 \cdot 7 + 5$ requires

$$a_2^{7^{n-1} + 7^{n-2} + \dots + 7^2} \{ 2a_4^9 + 4a_2 a_4^7 a_6 + 6a_2^2 a_4^8 + a_2^4 a_4^7 + 4a_2^7 a_4 a_6^3 + a_2^7 a_4^4 a_6 \\ + 6a_2^8 a_4^2 a_6^2 + 2a_2^9 a_6^3 + 2a_2^{15} a_6 + a_2^{14} a_4^2 + 3a_2^{16} a_4 + 4a_2^{18} \} = 0,$$

the last four terms not occurring when $n = 2$.

Applying (1) to eliminate a_6 ,

$$4a_4^8 + 4a_2^2 a_4^7 + a_2^4 a_4^6 + 2a_2^6 a_4^5 + 2a_2^8 a_4^4 + 5a_2^{10} a_4^3 + 2a_2^{14} a_4 + 4a_2^{16} = 0, \quad (4)$$

the last two terms not occurring when $n = 2$.

For $n = 2$, we may give (4) the form

$$4a_4^3(a_4 - 2a_2^2)(a_4 - 4a_2^2)(a_4 - 5a_2^2)[a_4 - (1 + \sqrt{3})a_2^2][a_4 - (1 - \sqrt{3})a_2^2] = 0.$$

But by (3)

$$(a_2a_4)^8 = -2^2 = 3.$$

Hence a_2 is a not-square in the $GF[7^2]$ and

$$a_4 = \pm 2a_2^2.$$

Thus $(\pm 2)^8 = 4$; $4^8 = 2$; $(1 \pm \sqrt{3})^8 = 5$, each modulo 7.

For $n > 2$, (4) may be written

$$4(a_4 + 2a_2^2)^5(a_4^3 - 2a_4^2a_2^2 + 3a_4a_2^4 + 2a_2^6) = 0, \quad (4')$$

the last factor being irreducible in the $GF[7^1]$.

By using § 68, I find that the power

$$7^{n-1} + 2 \cdot 7^{n-2} + \dots + 2 \cdot 7^2 + 3 \cdot 7 + 2$$

gives for $n > 2$ a condition of six terms which on applying (1) to eliminate a_6 reduces to an identity. But the power $7^{n-1} + 2 \cdot 7^{n-2} + \dots + 2 \cdot 7^2 + 3 \cdot 7 + 4$ requires for $n > 2$

$$\begin{aligned} a_2^{7^{n-1} + \dots + 7^2} \{ & 4a_2a_6^8a_4^7 + 2a_6^7a_4^9 + 4a_2^2a_6^7a_4^8 + 6a_2^7a_6^{10}a_4 + 5a_2^4a_6^7a_4^7 + 3a_6^3a_4^{15} \\ & + 2a_2^{15}a_6^8 + a_2^{14}a_6^7a_4^2 + 2a_2^8a_6a_4^{14} + a_2^7a_4^{16} + 2a_2^{16}a_6^7a_4 + 2a_2^9a_4^{15} \\ & + 6a_2^{18}a_6^7 + 3a_2^{14}a_6^3a_4^8 + 6a_2^{11}a_4^{14} \} = 0. \end{aligned}$$

Applying (1) to eliminate a_6 (the 4th, 6th and 14th terms cancel),

$$a_4^7 \{ 6a_4^{15} + a_2^2a_4^{14} + 3a_2^{14}a_4^8 + 4a_2^{16}a_4^7 + 3a_2^{28}a_4 + 4a_2^{30} \} = 0,$$

or

$$a_4^7(a_4 + 6a_2^2)(a_4 + 2a_2^2)^{14} = 0.$$

Hence by (4') the only possible values, when $n > 2$, are

$$a_4 = -2a_2^2, \quad a_6 = -a_2^3.$$

The same holds also for $n = 2$, since the set of values

$$a_4 = +2a_2^2, \quad a_6 = 4a_2^3$$

is excluded by the condition, given by the 18th power,

$$\begin{aligned} a_2a_4^7 + 3a_2^7a_4a_6^2 + 5a_2^9a_6^2 + 3a_2^8a_4^2a_6 + 2a_2^7a_4^4 + 4a_2^{15} + 3a_2a_4^7a_6^8 \\ + 5a_4^9a_6^7 + 3a_2^2a_4^8a_6^7 + a_2^7a_4a_6^{10} + 2a_2^4a_4^7a_6^7 + 4a_4^{15}a_6^3 = 0, \end{aligned}$$

which reduces to $6a_2^{15} = 0$ by substituting the latter set of values, is an identity for

$$a_4 = -2a_2^2, \quad a_6 = -a_2^3.$$

The only possible form is thus $\xi(\xi^2 - 2a_2)^3$, which may be proved suitable on 7^n letters, if $2a_2$ be a not-square, by the method used in § 39 or as below.

74. $p^r = 11$.

(a) $\xi^{11} + a_{10}\xi$.

Suitable if $-a_{10}$ be a not-tenth power in the $GF[11^n]$.

(b) $\xi^{11} + a_9\xi^2, a_9 \neq 0$.

The power $3 \cdot 11^{n-1} + 7(11^{n-2} + \dots + 11) + 9$ requires $a_9 = 0$.

(c) $\xi^{11} + a_8\xi^3 + a_{10}\xi, a_8 \neq 0$.

For the power $2 \cdot 11^{n-1} + 6(11^{n-2} + \dots + 11) + 8$, we must have $s = 11^n - 1$ and then $a_0 \leq 6(11^{n-2} + \dots + 11) + 8$. We may prove by induction that

$$a_0 \leq 4(11^{n-2} + 11^{n-3} + \dots + 11) + 8.$$

Thus suppose

$$a_0 = 4(11^{n-2} + 11^{n-3} + \dots + 11^{n-k}) + 6(11^{n-k-1} + \dots + 11) + 8 - x,$$

$$0 \leq x \leq 11^{n-k-1} + 6(11^{n-k-2} + \dots + 11) + 8.$$

Then

$$a_3 + a_{10} = 2 \cdot 11^{n-1} + 2 \cdot 11^{n-2} + \dots + 2 \cdot 11^{n-k} + x.$$

If $a_8 = 2 \cdot 11^{n-1} + \dots + 2 \cdot 11^{n-k} + y$, where $0 \leq y \leq x$,

$$s = 11^n + 11^{n-k} + 6(11^{n-k-1} + \dots + 11^2) + 8 \cdot 11 - 10x + 2y > 11^n.$$

If $a_8 = 2 \cdot 11^{n-1} + \dots + 2 \cdot 11^{n-k+1} + 11^{n-k} + y$,

$$s = 10(11^{n-1} + \dots + 11^{n-k+1} + 11^{n-k}) + 6(11^{n-k-1} + \dots + 11^2) + 8 \cdot 11 - 10x + 2y < 11^n - 1.$$

Hence

$$a_0 < 4(11^{n-2} + \dots + 11^{n-k}) + 5 \cdot 11^{n-k-1}$$

and thus

$$\leq 4(11^{n-2} + \dots + 11^{n-k-1}) + 6(11^{n-k-2} + \dots + 11) + 8.$$

It is now easily shown that

$$a_0 = 4(11^{n-2} + \dots + 11 + 1), \quad a_3 = 2 \cdot 11^{n-1} + \dots + 2 \cdot 11 + 3, \quad a_{10} = 1,$$

as a smaller value for a_0 would require $s < 11^n - 1$. The condition is thus

$$a_8^{2 \cdot 11^{n-1} + \dots + 2 \cdot 11 + 3} a_{10} = 0 \quad \text{or} \quad a_{10} = 0.$$

The power $2 \cdot 11^{n-1} + 6(11^{n-2} + \dots + 11) + 10$ then requires that $a_8 = 0$.

(d) $\xi^{11} + a_7 \xi^4 + a_9 \xi^2 + a_{10} \xi, a_7 \neq 0$.

The powers $11^{n-1} + 7(11^{n-2} + \dots + 11) + 9$, $11^{n-1} + 7(11^{n-2} + \dots + 11) + 10$, and $2 \cdot 11^{n-1} + 4(11^{n-2} + \dots + 11) + 8$, require in turn,

$$a_9 = 0, \quad a_{10} = 0, \quad a_7 = 0.$$

(e) $\xi^{11} + a_6 \xi^5 + \dots$ is rejected by § 66.

(f) $\xi^{11} + a_5 \xi^6 + a_7 \xi^4 + a_8 \xi^3 + a_9 \xi^2 + a_{10} \xi, a_5 \neq 0$.

The power $11^{n-1} + 5(11^{n-2} + \dots + 11) + 6$ requires $a_7 = 0$.

The powers $11^{n-1} + 5(11^{n-2} + \dots + 11) + 7$ and $11^{n-1} + 5(11^{n-2} + \dots + 11^2) + 6 \cdot 11 + 4$ require respectively

$$a_5^{11^{n-1} + \dots + 11 + 1} (a_9^2 + 2a_8 a_{10} + 5a_5^2 a_8) = 0$$

$$a_5^{11^{n-1} + \dots + 11 + 1} a_8^{11} (a_9^2 + 2a_8 a_{10} + 4a_5^2 a_8) = 0.$$

Hence $a_8 = 0$ and then $a_9 = 0$.

The power $11^{n-1} + 5(11^{n-2} + \dots + 11) + 9$ of $\xi^{11} + a_5 \xi^6 + a_{10} \xi$ requires

$$a_5^{11^{n-1} + \dots + 11 + 1} (a_{10} - 3a_5^2) = 0.$$

The only possible form is thus $\xi (\xi^5 - 5a_5)^2$.

(g) The cases $a_2 \neq 0, a_3 \neq 0, a_4 \neq 0$ I have not attempted. $a_1 = 0$ by § 65.

75. Theorem.* *If d be any divisor of $p^r - 1$, the quantic*

$$\xi (\xi^d - \nu)^{(p^r - 1)/d},$$

where ν is a not d th power in the $GF[p^n]$, represents a substitution on its p^n marks.

We are to show that

$$\xi (\xi^d - \nu)^{(p^r - 1)/d} = \beta \tag{1}$$

has a solution ξ belonging to the $GF[p^n]$, β being an arbitrary mark of that field. The statement being evident when $\beta = 0$, we will suppose that $\beta \neq 0$. Writing $\varphi = \xi^d - \nu$ our quantic becomes

$$\varphi^{(p^r - 1)/d} \cdot (\varphi + \nu)^{1/d} = (\varphi^{p^r} + \nu \varphi^{p^r - 1})^{1/d}.$$

It is then sufficient to prove that

$$\varphi^{p^r} + \nu \varphi^{p^r - 1} = \beta^d = \delta \tag{2}$$

* From the results of §§ 70, 72, 73, and 74, for $p = 3, 5, 7$ and 11, respectively, I venture the conjecture that all substitution quantics of degree p suitable on p^n letters are reducible to the simple type

$$\xi (\xi^d - \nu)^{(p - 1)/d}$$

where d is a divisor of $p - 1$.

has a solution φ belonging to the $GF[p^n]$, δ being any d th power and ν any not d th power of the field. For if there be such a solution φ (which $\neq 0$, since $\beta \neq 0$), then

$$\xi = (\varphi + \nu)^{1/d} = \beta/\varphi^{(p^n-1)/d}$$

will belong to the $GF[p^n]$ and satisfy (1).

Writing in (2)

$$\varphi = 1/\omega$$

and multiplying by ω^{ν^r} , we obtain

$$1 + \nu\omega = \delta\omega^{\nu^r}.$$

If we make

$$\delta\delta' = 1, \quad \nu\delta' = \nu',$$

δ' being thus a d th power and ν' a not d th power in the field, the last equation becomes

$$\omega^{\nu^r} - \nu'\omega = \delta'.$$

But this always has a solution in the field; for by § 57, corollary, the quantic

$$\omega^{\nu^r} - \nu'\omega$$

represents a substitution on p^n letters, ν' being a not d th power and hence a not $(p^n - 1)$ st power, d being a divisor of $p^n - 1$.

For $r = n$, this theorem is a special case of the following theorem:*

76. *If r is prime to and $< p^n - 1$, if s is a divisor of $p^n - 1$, and if $f(\xi^s)$ is a rational integral function of ξ^s belonging to the $GF[p^n]$ which can never vanish, then the quantic*

$$\xi^r [f(\xi^s)]^{(p^n-1)/s}$$

represents a substitution on p^n letters.

For if the quantic be raised to the l th power, l being not divisible by s , we have a set of terms whose exponents are of the form $ms + lr$ and thus are not divisible by s and hence not by $p^n - 1$. But if

$$l = ts < p^n - 1,$$

we get the term ξ^{ν^r} , since by the hypothesis on $f(\xi^s)$ we have

$$[f(\xi^s)]^{\nu^{n-1}} = 1.$$

But lr is not divisible by $p^n - 1$.

* Proved for $n = 1$ by Rogers, l. c. p. 41. I give a modified proof.

77. The substitution quantics given by § 76 and, when $n \leq r$, by § 75 are not reduced.

Thus, for $p > 2$, we have the suitable quantic

$$\xi^r (\xi^{\frac{p^n-1}{2}} - \nu)^2 = -2\nu \{ \xi^{\frac{p^n-1}{2}+r} - 1/2 (\nu + 1/\nu) \xi^r \}$$

ν being a not $(p^n - 1)/2$ power in the $GF[p^n]$ and thus any mark except $+1, -1, 0$. For the $p^n - 3$ values of ν , we get for each value of r , $(p^n - 3)/2$ different substitution quantics on p^n letters. For if

$$\nu + 1/\nu = \nu' + 1/\nu'$$

then either $\nu = \nu'$ or $\nu = 1/\nu'$. Also $\nu \neq 1/\nu$.

Examples of the above quantic:

$n = 1, p = 5$: ξ^3 and ξ .

$n = 1, p = 7$: $\xi^4 \pm 3\xi$ and $\xi_5 \pm 2\xi^2$, Hermite's forms.

$n = 1, p = 11$: $\xi^6 \pm 2\xi$, $\xi^6 \pm 4\xi$ (see § 45).

$n = 2, p = 3$: $\xi, \xi^3, \xi^5, \xi^5 \pm 2^{1/2}\xi$ (see § 44).

For the values $n = 1, p = 7$, we have if $\nu^3 = -1$,

$$\xi (\xi^2 - \nu)^3 = -3\nu (\xi^5 - \nu\xi^3 + 3\nu^2\xi)$$

$$\xi^5 (\xi^2 - \nu)^3 = 2 \{ \xi^5 + 2\nu\xi^3 + 3(2\nu)^2\xi \}$$

which together give the known quantic on 7 letters,

$$\xi^5 + a\xi^3 + 3a^2\xi, \quad a = \text{arbitrary.}$$

SECTION IV.—Degree a multiple, but not a power, of p .

78. Attempting no general investigation, I will confine myself to the determination of all *sextics* suitable on 3^n letters, together with a few special results on *sextics* suitable on 2^n letters.

$\varphi(\xi) = \xi^6 + a_1\xi^5 + a_2\xi^4 + a_3\xi^3 + a_4\xi^2 + a_5\xi$ on 3^n letters, §§ 79–82

79. Applying a linear transformation (in the $GF[3^n]$),

$$\begin{aligned} \varphi(\xi + \eta) = & \xi^6 + a_1\xi^5 + (a_2 + 2a_1\eta)\xi^4 + (a_3 + a_2\eta + a_1\eta^2 + 2\eta^3)\xi^3 \\ & + (a_4 + a_1\eta^3)\xi^2 + (a_5 + 2a_4\eta + a_2\eta^3 + 2a_1\eta^4)\xi + \varphi(\eta). \end{aligned}$$

Hence if $a_1 \neq 0$, either the coefficient of ξ^4 or that of ξ^2 can be removed by choice of η . But if $a_1 = 0$, no other coefficient can be removed in general by a linear transformation.

80. The case $a_1 = 0$.

(a) $n = 2$.

The second, fourth and fifth powers require respectively,

$$a_4 = a_2^2 \quad (1)$$

$$1 + a_2^4 + a_4^4 = 0 \quad (2)$$

$$a_2^3 + 2a_2a_4 + a_2^3 + 2a_3^3a_5 + 2a_2^3a_3a_5 + a_2^3a_4^2 + 2a_2a_3^4 + 2a_2a_5^4 + 2a_2a_4^3 \\ + 2a_3a_4a_5^3 + a_4^3a_5^2 = 0. \quad (3)$$

The seventh power requires exactly the cube of (3).

From (1) and (2), a_2 is a square $\neq 0$ in the $GF[3^2]$.

From (1) and (3),

$$(a_3^2 + 2a_2^3a_3a_5 + a_2^6a_5^2) + 2(a_5 + a_2a_3)(a_3^3 + a_2a_5^3) = 0.$$

Multiplying by a_2^3 and applying $a_2^4 = 1$,

$$(a_5 + a_2a_3)^2 \{a_2 + 2(a_5 + a_2a_3)^2\} = 0.$$

Hence either

$$a_5 = 2a_2a_3 \text{ or } a_5 = 2a_2a_3 \pm a_2^{1/2}.$$

The case $a_5 = 2a_2a_3$ is excluded below. The quantic

$$\xi^6 + a_2\xi^4 + a_3\xi^3 + a_2^2\xi^2 + (2a_2a_3 \pm a_2^{5/2})\xi \quad (4)$$

becomes by writing $\xi = \pm a_2^{1/2}\eta$, $a_3 = \pm a_2^{3/2}a$,

$$a_2^3 \{ \eta^6 + \eta^4 + a\eta^3 + \eta^2 + (2a + 1)\eta \}.$$

The resultant of the equations

$$\eta^6 + \eta^4 + a\eta^3 + \eta^2 + (2a + 1)\eta = 0; \quad \eta^5 = 1$$

is

$$a^5 - a^4 + a^2 + 1 = (a + 1)(a^2 - a - 1)^2.$$

Hence a may have any value in the $GF[3^2]$ except 2 and $2 \pm 2^{1/2}$.

The ultimately reduced form of (4)

$$\xi^6 + \xi^4 + a\xi^3 + \xi^2 + (2a + 1)\xi$$

represents the following substitutions on the marks of the $GF[3^2]$:

(0) (1) (-1) $(2^{1/2}, 2^{1/2} - 1, 2^{1/2} + 1)$ $(-2^{1/2}, -2^{1/2} - 1, -2^{1/2} + 1)$ for $a = 0$.

(0) (1) (-1) $(2^{1/2}, -2^{1/2} - 1, 2^{1/2} + 1, -2^{1/2}, 2^{1/2} - 1, -2^{1/2} + 1)$ for $a = 1$.

(0) (1) (-1) $(-2^{1/2})$ $(-2^{1/2} + 1)$ $(-2^{1/2} - 1)$ $(2^{1/2}, 2^{1/2} + 1, 2^{1/2} - 1)$ for $a = 2^{1/2}$.

(0) (1) (-1) $(2^{1/2}, -2^{1/2} + 1, 2^{1/2} + 1, -2^{1/2} - 1, 2^{1/2} - 1, -2^{1/2})$ for $a = 1 + 2^{1/2}$.

(b) $n > 2$. Write $3^n = 6m + 3$, m being thus of the form $9k + 4$.

The powers $m + 1$, $m + 3$, and $m + 4$ require respectively

$$a_4 = a_2^2 \quad (1)$$

$$a_4(2a_4^3 + a_2^6) = 0$$

$$\begin{aligned} a_3a_5^4 + a_3a_4a_5^3 + 2a_4^3a_5^2 + a_2^3a_4^4 + 2a_3^6a_4 + a_2^6a_2^5 + 2a_2^5a_4^3 + a_2^4a_3^3a_5 \\ + a_2^3a_3^4a_4 + a_2^2a_3^6 + 2a_2^9a_4 + a_2^{11} = 0, \quad (2) \end{aligned}$$

the last two terms not occurring when $n = 3$.

Applying (1) to (2), we have whether $n \geq 3$,

$$a_2(a_5^4 + a_2a_3a_5^3 + a_2^3a_3^3a_5 + a_2^4a_3^4) = a_2(a_5 + a_2a_3)^4 = 0.$$

Consider the power $3^{n-1} + 3^{n-2} + \dots + 3 + 1 = a_0 + a_2 + a_3 + a_4 + a_5$.

For $s = 6a_0 + 4a_2 + 3a_3 + 2a_4 + a_5 = 3(3^n - 1)$, we have

$$a_0 = 3^{n-1} + \dots + 3 + 1, \quad a_2 = a_3 = a_4 = a_5 = 0.$$

For $6a_0 + 4a_2 + 3a_3 + 2a_4 + a_5 = 2(3^n - 1) = 3^n + 2 \cdot 3^{n-1} + 2 \cdot 3^{n-2} + \dots + 2 \cdot 3 + 1$, it follows that $a_4 = 0$. For, in the notation of § 73 (f), if $c_j^{(4)} = 1$, then $c_{j+1}^{(4)} = 1, \dots, c_{n-1}^{(4)} = 1$; while $a_4 > 3^{n-1}$ would give $s < 2(3^n - 1)$. Also $a_5 = 0$; for if $c_r^{(5)} = 1$, then $c_{r+1}^{(4)} = 1$.

Thus $2a_0 - a_3 = 0$, or $a_0 = a_3 = 0$, $a_2 = 3^{n-1} + \dots + 3 + 1$.

For $s = 3^n - 1$, we have at once

$$a_4 = 3^{n-1} + 3^{n-2} + \dots + 3 + 1, \quad a_0 = a_2 = a_3 = a_5 = 0.$$

The condition is thus

$$1 + a_2^{3^{n-1}+\dots+3+1} + a_4^{3^{n-1}+\dots+3+1} = 0.$$

Hence by (1), a_2 is a square $\neq 0$ in the $GF[3^n]$.

The only possible form is thus

$$\xi^6 + a_2 \xi^4 + a_3 \xi^3 + a_2^2 \xi^2 + 2a_2 a_3 \xi,$$

which is *not* suitable on 3^n letters since it vanishes for $\xi = a_2^{1/2} \neq 0$.

81. The case $a_1 \neq 0$. Removing the term a^4 , we consider

$$\xi^6 + a_1 \xi^5 + a_3 \xi^3 + a_4 \xi^2 + a_5 \xi.$$

(a) $n = 2$. The second, fourth and fifth powers require respectively,

$$a_4 = 2a_1 a_3. \quad (1)$$

$$1 + a_1^3 a_5 + a_1 a_5^3 + a_4^4 = 0. \quad (2)$$

$$a_3^2 + 2a_1 a_5 + 2a_1^3 a_3 + 2a_3^3 a_5 + a_1^2 a_4^3 + 2a_1 a_3^3 a_4 + 2a_3 a_4 a_5^3 + a_4^3 a_5^2 = 0. \quad (3)$$

The seventh power requires the cube of (3).

First, $a_4^8 = 1$. For if $a_4 = 0$, then $a_3 = 0$ by (1) and then $a_5 = 0$ by (3), which is contrary to (2).

By squaring (2),

$$\begin{aligned} a_1^6 a_5^2 + 2a_1^4 a_5^4 + a_1^2 a_5^6 &= a_4^8 + 2a_4^4 + 1 = 2(a_4^4 + 1) \\ &= a_1^3 a_5^{-1} + a_1 a_5^3. \end{aligned} \quad (2')$$

But $a_5 \neq 0$; for if $a_5 = 0$, then by (3)

$$a_1^6 (a_3^2 + 2a_1^3 a_3 + 2a_1^5 a_3^3 + a_1^2 a_3^4) = a_3 (a_3 - a_1^3) (a_3^2 + a_1^6) = 0.$$

If either $a_3 = a_1^3$ or $a_3 = 2^{1/2} a_1^3$, then by (1) $a_4^4 = 1$, contrary to (2) for $a_5 = 0$.

Hence by (2')

$$a_1^5 a_5 + 2a_1^3 a_5^3 + a_1 a_5^5 + 2a_1^2 + 2a_5^2 = 0.$$

Writing $a_5 = \gamma a_1^5$ this becomes, aside from the factor a_1^2 ,

$$(\gamma + 1)(\gamma^2 + 1)(\gamma^2 - \gamma - 1) = 0.$$

If $\eta = -1$, $a_4^4 = 1$ by (2), while (3) becomes

$$a_1^6 + 2a_1^3a_3 + 2a_1^5a_3^3 + a_1^2a_3^4 = a_1^2(a_3 - a_1^3)^4 = 0.$$

The resulting quantic

$$\xi^6 + a_1\xi^5 + a_1^3\xi^3 - a_1^4\xi^2 - a_1^5\xi$$

is suitable on 3^2 letters. Thus for $a_1 = 1$, it represents the following substitution on the marks of the $GF[3^2]$:

$$(0)(1)(-1)(2^{1/2}, -2^{1/2})(2^{1/2} + 1, -2^{1/2} - 1, -2^{1/2} + 1, 2^{1/2} - 1).$$

If $\eta^2 = -1$, $a_5 = 2^{1/2}a_1^5$, while (2) and (3) become

$$a_4^4 = -1;$$

$$(1 - 2^{1/2})a_3^2 - 2^{1/2}a_1^6 + 2a_1^3a_3 - 2^{1/2}a_3^3a_1^5 + a_1^2a_3^4 = 0.$$

Multiplying by a_1^2 , and placing $a_1^4a_3^4 = a_4^4 = -1$, $a_3 = \varphi a_1^3$,

$$-2^{1/2}\varphi^3 + (1 - 2^{1/2})\varphi^2 + 2\varphi - (1 + 2^{1/2}) = 0,$$

whose roots are

$$1 - 2^{1/2}, -1 - 2^{1/2}, -1 + 2^{1/2}.$$

But $\xi^6 + a_1\xi^5 + \varphi a_1^3\xi^3 - \varphi a_1^4\xi^2 + 2^{1/2}a_1^5\xi$ vanishes for $\xi = -2^{1/2}a_1$ when $\varphi = -1 - 2^{1/2}$, while for $\varphi = 1 - 2^{1/2}$ or $\varphi = -1 + 2^{1/2}$ it represents a substitution on the marks of the $GF[3^2]$. Thus, taking $a_1 = 1$,

$$\xi^6 + \xi^5 + (1 - 2^{1/2})\xi^3 - (1 - 2^{1/2})\xi^2 + 2^{1/2}\xi,$$

$$\xi^6 + \xi^5 + (-1 + 2^{1/2})\xi^3 - (-1 + 2^{1/2})\xi^2 + 2^{1/2}\xi,$$

represent respectively the substitutions

$$(0)(-1, 2^{1/2} + 1)(1, 2^{1/2} - 1, -2^{1/2}, -2^{1/2} - 1, 2^{1/2}, -2^{1/2} + 1)$$

$$(0)(-1)(1, 2^{1/2} - 1, 2^{1/2})(2^{1/2} + 1, -2^{1/2}, -2^{1/2} + 1, -2^{1/2} - 1).$$

If $\eta^2 = \eta + 1$, $a_5 = (2^{1/2} - 1)a_1^5$, and (2) and (3) become

$$a_4^4 = 1$$

$$-2^{1/2}a_3^2 + (1 - 2^{1/2})a_1^6 + 2a_1^3a_3 + 2^{1/2}a_1^5a_3^3 + a_1^2a_3^4 = 0.$$

Multiplying by a_1^2 and placing $a_1^4 a_3^4 = a_4^4 = 1$, $a_3 = \varphi a_1^3$

$$2^{1/2} \varphi^3 - 2^{1/2} \varphi^2 - \varphi - (2^{1/2} + 1) = 0.$$

Its roots are $-1, 1 \pm (-2^{1/2} - 1)^{1/2}$, of which the last two are not marks of the $GF[3^2]$ since $(-2^{1/2} - 1)^4 = -1$.

The quantic given by $\varphi = -1$,

$$\xi^6 + a_1 \xi^5 - a_1^3 \xi^3 + a_1^4 \xi^2 + (2^{1/2} - 1) a_1^5 \xi$$

represents when $a_1 = 1$ the substitution on the marks of the $GF[3^2]$:

$$(0) (2^{1/2}) (2^{1/2} - 1) (-2^{1/2} + 1) (1, 2^{1/2} + 1, -1, -2^{1/2}, -2^{1/2} - 1).$$

(b) $n = 3$.

The fifth, seventh, eighth and thirteenth powers require respectively,

$$a_4 + a_1 a_3 + a_1^4 = 0. \quad (1)$$

$$a_1 a_5^3 + a_4^4 + a_1^4 a_4^3 + a_1^3 a_3^3 a_4 = 0. \quad (2)$$

$$a_3 a_4 a_5^3 + 2a_4^3 a_5^2 + a_1^3 a_4 a_5^3 + a_1 a_3^3 a_4^3 + 2a_3^6 a_4 + a_1^4 a_3 a_5^3 + 2a_1^3 a_3^3 a_5^2 \\ + a_1^3 a_3 a_4^4 + 2a_1 a_3^7 = 0. \quad (3)$$

$$1 + a_1^9 a_4^3 a_5 + a_1^3 a_4 a_5^9 + a_1 a_4^9 a_5^3 + a_4^{13} = 0. \quad (4)$$

The tenth power gives an identity; the eleventh requires exactly the 9th power of (2).

Applying (1) to (2)

$$a_1 (a_5^3 + 2a_1^6 a_3^3 + a_1^{12} a_3) = 0$$

or

$$a_5 = a_1^2 a_3 + 2a_1^4 a_3^9. \quad (5)$$

(b₁) If $a_3 = 0$, then $a_5 = 0$, $a_4 = -a_1^4$ and the sextic obtained, $\xi^6 + a_1 \xi^5 - a_1^4 \xi^2$ is suitable on the mark of the $GF[3^3]$. Thus $\xi^6 + \xi^5 - \xi^2$ represents the substitution

$$(0) (1) (-1) (j, j^2 - 1, -j^2 + j - 1, -j^2 + j + 1, j - 1, j^2 + j, -j^2, \\ -j^2 - 1, j + 1, j^2 - j, -j^2 - j - 1, -j^2 - j + 1) (-j, -j^2 + j, \\ j^2, j^2 + j - 1, -j - 1, -j^2 - j, j^2 - j + 1, j^2 + 1, -j + 1, \\ -j^2 + 1, j^2 + j + 1, j^2 - j - 1),$$

where $j^3 = j + 1$ is the irreducible equation defining the $GF[3^3]$.

(b₂) If $a_3 \neq 0$, we have on applying (1) and (5) to (3),

$$a_1^{13}a_3(2a_1^6 + 2a_3^2 + a_1^5a_3^9 + a_1^7a_3^{17}) = 0.$$

Writing $a_3 = \eta a_1^3$, this becomes

$$\eta^{17} + \eta^9 - \eta^2 - 1 = 0.$$

Multiply by η^9 , replace η^{11} by η^{11+52} and η^{26} by 1:

$$1 - \eta^{18} - \eta^{63} - \eta^{11} = 0.$$

Extracting the ninth root,

$$1 + \eta^2 - \eta^7 - \eta = -(\eta - 1)^2(\eta^2 + 1)(\eta^3 - \eta^2 - \eta - 1) = 0.$$

Now $\eta = 1$ is excluded since $\xi^6 + a_1\xi^5 + a_1^3\xi^3 + a_1^4\xi^2$ vanishes for $\xi = -a_1$.

Again $\eta^2 \neq -1$, since then $\eta^{26} = -1$.

If $\eta^3 = \eta^2 + \eta + 1$, then $\eta^9 = -\eta^2 + \eta$, $\eta^{13} = 1$.

From (1) and (5)

$$a_3 = \eta a_1^3, a_4 = -(\eta + 1)a_1^4, a_5 = (\eta + 2\eta^9)a_1^5 = \eta^2 a_1^5.$$

Substituting these values in (4), using $\eta^{13} = 1$, we have

$$-\eta^{12} - \eta^{10} - \eta^9 + \eta^6 + \eta^5 - \eta^4 - \eta^3 + \eta^2 - \eta - 1 = 0.$$

which is readily seen to be inconsistent with

$$\eta^3 = \eta^2 + \eta + 1.$$

(c) $n > 3$. Write $3^n = 6m + 3$.

The powers $m + 1$ and $m + 2$ require respectively,

$$a_4 + a_1a_3 + a_1^4 = 0$$

$$a_1a_5^3 + a_4^4 + a_1^4a_4^3 + a_1^3a_3^3a_4 + a_1^{12}a_4 + 2a_1^{16} = 0.$$

From these

$$a_1(a_5^3 + 2a_1^6a_3^3 + a_1^{15}) = 0$$

or

$$a_5 = a_1^2a_3 + 2a_1^5.$$

But

$$\xi^6 + a_1\xi^5 + a_3\xi^3 - (a_1a_3 + a_1^4)\xi^2 + (a_1^2a_3 + 2a_1^5)\xi$$

vanishes for $\xi = -a_1$ and is thus excluded.

82. Summary of §§ 79-81. The only reduced $SQ[6; 3^n]$ are the last five quantities in the table § 87.

Introductory study of sextics on 2^n letters, §§ 83.

83. If $\varphi(\xi) \equiv \xi^6 + a_1\xi^5 + a_2\xi^4 + a_3\xi^3 + a_4\xi^2 + a_5\xi$, then

$$\begin{aligned} \varphi(\xi + \eta) = \xi^6 + a_1\xi^5 + (\eta^2 + a_1\eta + a_2)\xi^4 + a_3\xi^3 + (\eta^4 + a_3\eta + a_4)\xi^2 \\ + (a_1\eta^4 + a_3\eta^2 + a_5)\xi + \varphi(\eta). \end{aligned}$$

Hence in general no term can be removed. If $a_1 = 0$ we can make the coefficient of ξ^4 zero; if $a_3 = 0$, we can make that of ξ^2 zero.

84. The case n even. Then $2^n = 6m + 4$.

(a) $n = 4$. Of the "power conditions," two are independent,

$$a_3 = a_1^3 \mp 0.$$

$$\begin{aligned} a_2a_5^2 + a_4^3 + a_3^4 + a_2^4a_4 + a_1^4a_4^2 + a_2^6 + a_1^4a_2^2a_4 + a_1^4a_2a_3^2 + a_1^2a_2^5 + a_1^2a_5^5 \\ + a_1a_3^2a_5^4 + a_1a_4^4a_5^2 + a_2^2a_3a_5^4 + a_3^4a_5^3 + a_3^2a_4^4a_5 + a_3a_4^6 = 0. \end{aligned}$$

(b) $n > 4$.

The power $m + 1$ requires $a_3 = a_1^3$. Applying this to the condition given by the power $m + 5$:

$$\begin{aligned} a_1^2a_5^5 + a_1^7a_5^4 + a_1^3a_2^2a_5^4 + a_1a_4^4a_5^2 + a_1a_2^8a_5^2 + a_1^9a_2^4a_5^2 + a_1^6a_4^4a_5 + a_1^{22}a_5 \\ + a_1^{14}a_2^4a_5 + a_1^3a_4^6 + a_1^3a_2^8a_4^2 + a_1^{27} + a_1^{11}a_2^4a_4^2 + a_1^{23}a_2^2 + a_1^{11}a_2^8 + a_1^7a_2^{10} = 0. \end{aligned}$$

By the method of proof used in (f) § 73, we find the power

$$2m + 1 = 2^{n-2} + 2^{n-4} + \dots + 2^2 + 1$$

requires

$$1 + a_3^{2m+1} = 0 \text{ or } a_3 \mp 0.$$

85. The case n odd. Then $2^n = 6m + 2$.

(a) $n = 3$. The third power requires

$$a_4 + a_2^2 + a_1^2a_2 + a_1a_5^2 + a_3^2a_5 + a_3a_4^2 = 0. \quad (13)$$

The fifth power requires exactly the 4th power of this.

(b) $n > 3$. The power $m + 2$ requires

$$a_1a_5^2 + a_3a_4^2 + a_3^2a_5 + a_2^4a_3 + a_1^6a_5 + a_1^5a_3^2 + a_1^4a_2^2a_3 + a_1^3a_2^4 = 0. \quad (1_3)$$

The power $m + 6$ requires for $n > 5$ and $n = 5$ respectively

$$(a_3 + a_1^3)(a_1^{16}a_2^8 + a_2^{16} + a_4^8) + (a_3^8 + a_1^{24})(a_1a_5^2 + a_3a_4^2 + a_3^2a_5) = 0. \quad (2)$$

$$a_4 + a_2^2 + a_1^2a_2 + a_4^8(a_3 + a_1^3) + a_3^8(a_1a_5^2 + a_3a_4^2 + a_3^2a_5) = 0. \quad (2_5)$$

The powers $m + 8$ and $m + 18$ lead to (1).

(b₁) Suppose $a_1 = 0$, so that by § 83 we can take $a_2 = 0$.

If $a_3 \mp 0$ and $n > 5$, then by (1) and (2) we find $a_4 = a_5 = 0$.

But $\xi^6 + a_3 \xi^3$ vanishes for $\xi = a_3^{1/3}$; while every mark in the $GF[2^n]$, n odd, is a cube by § 18.

If $a_3 \neq 0$, and $n = 5$, (1) and (2₅) give

$$a_4^2 = a_3 a_5; \quad a_4 = a_3^5 a_5^4.$$

Thus either $a_4 = a_5 = 0$, or $a_5 = a_3^{12}$, $a_4 = a_3^{22}$.

But $\xi^6 + a_3 \xi^3 + a_3^{22} \xi^2 + a_3^{12} \xi$ vanishes for $\xi = a_3^{21} = a_3^{1/3}$.

If $a_3 = 0$, then the power $2m + 1 = 2^{n-2} + 2^{n-4} + \dots + 2^3 + 2 + 1$ requires $a_4 = 0$. But $\xi^6 + a_5 \xi$ vanishes for $\xi = a_5^{1/5}$, a mark of the $GF[2^n]$, n odd.

Hence every suitable sextic on 2^n letters, n odd and 73, in which the coefficient of ξ^5 is zero, is reducible to the form ξ^6 .

(b₂) Suppose $a_3 = 0$, $a_1 \neq 0$. Then we may take $a_5 = 0$. Then $a_2 = 0$ by (1). For $n > 5$, $a_4 = 0$ by (2); for $n = 5$, (2₅) gives

$$a_4 + a_1^3 a_4^8 = 0,$$

hence either $a_4 = 0$ or $a_4 = a_1^4$.

But $\xi^6 + a_1 \xi^5$ vanishes for $\xi = a_1$ and is excluded.

The sextic $\xi^6 + a_1 \xi^5 + a_1^4 \xi^2$ represents a substitution on the marks of the $GF[2^5]$, viz, for $a_1 = 1$:

$$(0) \begin{aligned} & (j + 1, j^3 + j^2, j^2 + 1, j^4 + j^3 + j, j^4 + 1)(j^3 + j, j^4 + j^3 + 1, \\ & j^4 + j + 1, j^4 + j^3 + j^2 + 1)(j^3, j^4 + j^2 + j, j^4 + j^3 + j^2 + j, j^4 + j^2, \\ & j^3 + j^2 + j, j^2 + j)(j, j^3 + j + 1, j^4 + j^3 + j^2, j^2, j^3 + j^2 + j + 1, \\ & j^4 + j^2 + j + 1, j^4, j^4 + j^3 + j^2 + j + 1, j^4 + j^3, j^3 + j^2 + 1, j^4 + j, \\ & j^2 + j + 1, j^4 + j^3 + j + 1, j^3 + 1, j^4 + j^2 + 1), \end{aligned}$$

the $GF[2^5]$ being defined by the equation $j^5 = j^2 + 1$.

(b₃) Suppose $a_3 = a_1^3 \neq 0$. Then by (1)

$$a_5 = a_1^5 + a_1^3 a_2 + a_1 a_4.$$

(2) and (2₅) and (1₃) are seen to be satisfied; but

$$\xi^6 + a_1 \xi^5 + a_2 \xi^4 + a_1^3 \xi^3 + a_4 \xi^2 + (a_1^5 + a_1^3 a_2 + a_1 a_4) \xi$$

vanishes for $\xi = a_1$.

86. Summary of §§ 83–85. If a sextic represent a substitution on the marks of the $GF[2^n]$, then, for n even,

$$a_3 = a_1^3 \neq 0;$$

for n odd and > 3 ,

$$a_1 \neq 0, \quad a_3 \neq 0, \quad a_3 \neq a_1^3,$$

except for the suitable quantities

$$\xi^6 \text{ on } 2^n \text{ letters; } \xi^6 + a \xi^5 + a^4 \xi^2 \text{ on } 2^5 \text{ letters.}$$

87. *Table.**

Except for sextics on 2^n letters, the following is a complete list of all *reduced* quantics $\varphi(\xi)$ of degree ≤ 6 which are suitable to represent substitutions on a power of a prime number of letters. From them (by § 16) all suitable quantics whatsoever of degree ≤ 6 are obtained by the formula

Reduced quantic.	$a\varphi(\xi + \beta) + \gamma$.	Suitable for $p^n =$
ξ		any
ξ^2		2^n
ξ^3		$3^n, 3m + 2$
$\xi^3 - a\xi$ ($a =$ not-square)		3^n
$\xi^4 \pm 3\xi$		7
$\xi^4 + a_2\xi^2 + a_3\xi$		2^n
(when it vanishes only for $\xi = 0$)		
ξ^5		$5^n, 5m \pm 2, 5m + 4$
$\xi^5 - a\xi$ ($a =$ not 4th power)		5^n
$\xi^5 + 2^{1/2}\xi$		3^2
$\xi^5 \pm 2\xi^2$		7
$\xi^5 + a\xi^3 \pm \xi^2 + 3a^2\xi$ ($a =$ not-square)		7
$5\xi^2 + 5a\xi^3 + a^2\xi$ ($a =$ arbitrary)		$5m \pm 2$
$\xi^5 + a\xi^3 + 3a^2\xi$ ($a =$ not-square)		13
$\xi^5 + 2a\xi^3 + a^2\xi$ ($a =$ not-square)		5^n
ξ^6		$2^n, n$ odd.
$\xi^6 \pm 2\xi$		11
$\xi^6 \pm a^2\xi^3 + a\xi^2 \pm 5\xi$ ($a =$ square)		11
$\xi^6 \pm 4a^2\xi^3 + a\xi^2 \pm 4\xi$ ($a = 0$ or not-square)		11
$\xi^6 + a_2\xi^4 + a_3\xi^3 + a_2^2\xi_2 + (2a_2a_3 \pm a_2^5)\xi$		3^2
($a_2 =$ square $\neq 0$; $a_3 = 0, \pm 2^{1/2}a_2^{3/2}, \pm a_2^{3/2}$, or $\pm 2^{1/2} + 1$) $a_2^{3/2}$, the signs to correspond to that of $\pm a_2^{5/2}$).		
$\xi^6 + a\xi^5 - a^4\xi^2$ ($a =$ arbitrary)		$3^3, 2^5$
$\xi^6 + a\xi^5 + a^2\xi^3 - a^4\xi^2 - a^5\xi$ ($a =$ arbitrary)		3^2
$\xi^6 + a\xi^5 + \varphi a^3\xi^3 - \varphi a^4\xi^2 + 2^{1/2}a^5\xi$ ($a =$ arbitrary)		3^2
(where $\varphi = \pm (1 - 2^{1/2})$).		
$\xi^6 + a\xi^5 - a^3\xi^3 + a^4\xi^2 + (2^{1/2} - 1)a^5\xi$ ($a =$ arbitrary)		3^2

In this table $2^{1/2}$ occurs always as a symbol for *either* of the two marks of the $GF[3^2]$ satisfying the equation $x^2 - 2 = 0$.

88. Theorem. *All substitutions on 7 letters may be derived from the two*

$$x' = ax + b; x' = x^5.$$

$$\left[\begin{matrix} x \\ x + b \end{matrix} \right] \left[\begin{matrix} x \\ x^5 + b^5 \end{matrix} \right] \left[\begin{matrix} x \\ 3b^4x^5 + 2b^5 \end{matrix} \right] = \left[\begin{matrix} x \\ x^5 - b^2x^3 + b^3x^2 + 3b^4x \end{matrix} \right]; \quad (1)$$

* Compare *American Journal of Mathematics*, vol. 18, p. 218, § 19.

so that we reach the form

$$x^5 + ax^3 \pm x^2 + 3a^2x, \quad a = \text{quadratic non-residue of 7.}$$

$$\begin{aligned} \left[\begin{matrix} x \\ x - b^5 \end{matrix} \right] \left[\begin{matrix} x \\ x^5 \end{matrix} \right] \left[\begin{matrix} x \\ x^5 - b^2x^3 + b^3x^2 + 3b^4x \end{matrix} \right] \left[\begin{matrix} x \\ 5b^2x + 3b \end{matrix} \right] \\ = \left[\begin{matrix} x \\ x^5 - b^4x^3 + 3b^2x \end{matrix} \right]; \end{aligned} \quad (2)$$

so that by writing $b = c^5$ we reach the form

$$x^5 - c^2x^3 + 3c^4x.$$

$$\left[\begin{matrix} x \\ x^5 \end{matrix} \right] \left[\begin{matrix} x \\ x^5 - b^4x^3 + 3b^2x \end{matrix} \right] \left[\begin{matrix} x \\ 5b^4x \end{matrix} \right] = \left[\begin{matrix} x \\ x^5 + 2b^2x^3 + 3(2b^2)^2x \end{matrix} \right]. \quad (3)$$

Hence by (1) and (2) we reach the form

$$x^5 + ax^3 + 3a^2x, \quad a = \text{arbitrary.}$$

$$\left[\begin{matrix} x \\ x + 3b^5 \end{matrix} \right] \left[\begin{matrix} x \\ x^5 + b \end{matrix} \right] \left[\begin{matrix} x \\ x^5 - b^2x^3 + b^3x^2 + 3b^4x \end{matrix} \right] \left[\begin{matrix} x \\ b^3x + 2b^2 \end{matrix} \right] = \left[\begin{matrix} x \\ x^4 + 4b^3x \end{matrix} \right]; \quad (4)$$

so that we reach $x^4 \pm 3x$.

$$\left[\begin{matrix} x \\ x^5 \end{matrix} \right] \left[\begin{matrix} x \\ x^4 + 4b^3x \end{matrix} \right] \left[\begin{matrix} x \\ 2b^3x \end{matrix} \right] = \left[\begin{matrix} x \\ x^5 + 2b^3x \end{matrix} \right]; \quad (5)$$

so that we reach $x^5 \pm 2x$.

89. E. Betti proved (l. c. vol. 2, pp. 17-19, 1851) that all substitutions on 5 letters are derivable from

$$x' = ax + b; \quad x'' = x^3.$$

90. *Enumerative proof of Wilson's theorem.*

Of the $p!$ literal substitutions on a prime number p of letters, $p(p-1)$ have a linear representation

$$ax + b, \quad a \neq 0.$$

The remaining ones are represented by quantics of degree > 1 which fall into sets of $p^2(p-1)$ each, viz.

$$ac(x+b) + c, \quad a \neq 0, \quad b \text{ and } c \text{ arbitrary.}$$

Hence $p! - p(p-1)$ is a multiple of $p^2(p-1)$, so that $(p-1)! + 1$ is divisible by p .

END OF PART I.

THE ANALYTIC REPRESENTATION OF SUBSTITUTIONS ON A POWER OF A PRIME NUMBER OF LETTERS WITH A DISCUSSION OF THE LINEAR GROUP.

[CONTINUED.]

By DR. LEONARD EUGENE DICKSON, Chicago, Ill.

PART II.—LINEAR GROUPS.

SECTION I.—*Linear Homogeneous Group.*

1. We may define p^{nm} letters

$$l_{\xi_1, \xi_2, \dots, \xi_m}$$

characterized by m indices, each being an arbitrary mark of the Galois field of order p^n . The general *linear homogeneous substitution* A on these letters replaces $l_{\xi_1, \dots, \xi_m}$ by $l_{\xi'_1, \dots, \xi'_m}$, where

$$\xi'_i = \sum_{j=1}^m a_{ij} \xi_j \quad (i = 1, 2, \dots, m) \quad (1)$$

where the a_{ij} 's are marks of the $GF[p^n]$. But (1) will indeed be a substitution on the p^{nm} letters if and only if the determinant

$$A \equiv |a_{ij}| \neq 0. \quad (i, j = 1, 2, \dots, m)$$

For there must be one and only one system of m indices ξ_i which (1) replaces by a given system ξ'_i and hence an unique set of values ξ_j satisfying the equations

$$\sum_{j=1}^m a_{ij} \xi_j = \xi'_i. \quad (i = 1, \dots, m)$$

Remark. If the substitution (1) be identical with

$$\xi'_i = \sum_{j=1}^m a_{ij} \xi_j \quad (i = 1, \dots, m)$$

then must

$$\bar{a}_{ij} = a_{ij}. \quad (i, j = 1, 2, \dots, m)$$

This follows if we take in turn, for $j = 1, 2, \dots, m$, the particular set of values

$$\xi_j = 1; \xi_i = 0. \quad (i = 1, 2, \dots, m; i \neq j)$$

2. Let B denote a second linear homogeneous substitution

$$\xi'_j = \sum_{k=1}^m \beta_{jk} \xi_k \quad (j = 1, 2, \dots, m) \quad (2)$$

so that

$$|B| \equiv |\beta_{jk}| \neq 0.$$

The result of applying first the literal substitution

$$B = \begin{bmatrix} l_{\xi_i} \\ l_{\xi'_j} \end{bmatrix}$$

and afterwards the literal substitution

$$A = \begin{bmatrix} l_{\xi_i} \\ l_{\xi'_j} \end{bmatrix} = \begin{bmatrix} l_{\xi'_j} \\ l_{\xi''_j} \end{bmatrix},$$

where by (1)

$$\xi''_j = \sum_{l=1}^m a_{jl} \xi_l,$$

is the same as applying the single substitution

$$BA = \begin{bmatrix} l_{\xi'_j} \\ l_{\xi''_j} \end{bmatrix},$$

where

$$\xi''_j = \sum_{k=1}^m \gamma_{jk} \xi_k$$

if

$$\gamma_{jk} = \sum_{l=1}^m a_{jl} \beta_{lk}.$$

We may think of this compounding of two substitutions *analytically*. Laying aside the method of composition by matrices,* it will be found convenient here to think of the composition as follows. The result of applying the analytic substitution A first and B afterwards is denoted by BA . A replaces the index ξ_i by

$$\sum_{j=1}^m a_{ij} \xi_j,$$

* In the matrix notation the substitution (1) is denoted by (a_{ij}) . The composition formula is then

$$(a''_{ik}) = (a'_{ij})(a_{jk})$$

where

$$a''_{ik} = \sum_{j=1}^m a'_{ij} a_{jk},$$

provided the matrix (a_{jk}) operates first.

which in turn B replaces by

$$\sum_{j=1}^m a_{ij} \left[\sum_{k=1}^m \beta_{jk} \xi_k \right] \equiv \sum_{k=1}^m \gamma_{ik} \xi_k,$$

if

$$\gamma_{ik} = \sum_{j=1}^m a_{ij} \beta_{jk}.$$

The compound BA is indeed a substitution since

$$|BA| \equiv |\gamma_{ik}| \equiv |a_{ij}| \cdot |\beta_{jk}| \equiv |B| \cdot |A| \neq 0.$$

Moreover the γ_{ik} 's are marks of the $GF[p^n]$.

The literal substitution product $\overset{1}{B}\overset{2}{A}$ is thus the same as the analytic substitution compound $\overset{2}{B}\overset{1}{A}$. The transformed of T by S is always

$$S^{-1}TS.$$

For literal substitutions, S^{-1} operates first; while for analytic substitutions, S operates first. The result is the same in both cases.

It follows from the composition that the totality of linear homogeneous substitutions (1) forms a group, which is called the *linear homogeneous group of degree p^m* . It is a generalization of Jordan's linear homogeneous group* of degree p^m in which the m indices and m^2 coefficients are integral marks, i. e. marks of the $GF[p^1]$. It is however contained in the Jordan group on mn indices. It is identical† with the group investigated by E. Betti in 1852–1855 and in more detail by E. Mathieu in 1861.

3. Necessarily the group I study is of degree a power of a *prime*. But all that is of essential interest in Jordan's general linear homogeneous group of degree q^m centers in the case when q is a prime. Thus by Jordan, l. c. Arts. 127–131, the factors of composition of the linear group on m indices modulo q are simply the factors of composition of the groups on m indices taken respectively modulo $p_i^{r_i}$ where

$$q = \prod_{i=1}^t p_i^{r_i},$$

$p_1, p_2, \dots, p_t$ being the different prime factors of q . While by Arts. 132–134, the factors of composition of the group modulo $p_i^{r_i}$ are those of the group modulo p_i together with factors all equal to p_i . Hence for the study of non-cyclic *simple* linear groups the case of a composite modulus offers nothing beyond that of a prime modulus.

* Jordan, *Traité des Substitutions*, pp. 91–110, 1870.

† See Section III; also literature given in Preface.

4. Theorem.* *The order $\Omega(m, n, p)$ of the linear homogeneous group of degree p^{nm} on m indices is*

$$(p^{nm} - 1)(p^{nm} - p^n)(p^{nm} - p^{2n}) \dots (p^{nm} - p^{n(m-1)}).$$

Let N be the number of linear substitutions

$$R_1 = 1, R_2, R_3, \dots, R_N,$$

which leave the index ξ_1 invariable, and let T be a substitution which replaces it by

$$\sum_{j=1}^m \alpha_{1j} \xi_j.$$

The N substitutions

$$T, TR_2, TR_3, \dots, TR_N,$$

will replace ξ_1 by this same linear function, and no other substitution has this property; for if U were such a one, $T^{-1}U$ would leave ξ_1 invariable and hence be a certain R_k , so that

$$U = TR_k.$$

The marks α_{1j} may be taken arbitrary except that not all can be zero. Hence the system α_{1j} is susceptible of $p^{nm} - 1$ different sets of values. To each set correspond N substitutions. Hence

$$\Omega(m, n, p) = N(p^{nm} - 1).$$

But the substitutions R_k are of the form

$$\xi_1' = \xi_1; \xi_i' = \sum_{j=1}^m \alpha_{ij} \xi_j, \quad (i = 2, 3, \dots, m)$$

where the $m - 1$ coefficients α_{i1} are arbitrary and the coefficients $\alpha_{i2}, \alpha_{i3}, \dots, \alpha_{im}$ are such that their determinant is $\neq 0$, which can happen in $\Omega(m - 1, n, p)$ ways. Hence

$$N = p^{n(m-1)} \Omega(m - 1, n, p).$$

Thus

$$\begin{aligned} \Omega(m, n, p) &= p^{n(m-1)} (p^{nm} - 1) \Omega(m - 1, n, p) \\ &= p^{n(m-1)} (p^{nm} - 1) \cdot p^{n(m-2)} (p^{n(m-1)} - 1) \dots (p^n - 1) \\ &= (p^{nm} - 1) (p^{nm} - p^n) \dots (p^{nm} - p^{n(m-1)}), \end{aligned}$$

since evidently for a single index,

$$\Omega(1, n, p) = p^n - 1.$$

* Stated Jordan, l. c. Art. 169; proof for $n = 1$, Art. 123.

5. *Transformation of indices.* Let A be the linear homogeneous substitution on p^{nm} letters :

$$\xi'_i = \sum_{j=1}^m a_{ij} \xi_j. \quad (i = 1, 2, \dots, m) \quad (1)$$

We define m new quantities

$$\eta_i = \sum_{k=1}^m \beta_{ik} \xi_k \quad (i = 1, 2, \dots, m) \quad (2)$$

where the β_{ik} 's are marks of the $GF[p^n]$ such that

$$|B| \equiv |\beta_{ik}| \neq 0.$$

We may thus solve (2),

$$\xi_k = \sum_{i=1}^m \frac{B_{ik}}{|B|} \cdot \eta_i, \quad (k = 1, 2, \dots, m) \quad (3)$$

where B_{ik} denotes the adjoint of β_{ik} in $|\beta| \equiv |\beta_{ik}|$.

Instead of distinguishing the letters $\xi_1, \dots, \xi_m$ from each other by the variation of the indices ξ_i , we can distinguish then by the variation of the η_i 's considered as independent indices. Thus A will replace one of these new indices η_i by $\sum_{k,j} \beta_{ik} a_{kj} \xi_j$; so that, applying (3), we may write the substitution A

$$\eta'_i = \sum_{l=1}^m \gamma_{il} \eta_l \quad (i = 1, 2, \dots, m) \quad (4)$$

where

$$\gamma_{il} = \sum_{k,j} \beta_{ik} a_{kj} \cdot \frac{B_{lj}}{|B|}.$$

The coefficients β_{ik} may be chosen to simplify the expression of the substitution A .

Remark. The transformation of indices (2) leaves the determinant $|a_{ij}|$ of the substitution A invariant.

For, applying (2) to (4),

$$\sum_{k=1}^m \beta_{ik} \xi'_k = \sum_{l,k} \gamma_{il} \beta_{lk} \xi_k. \quad (i = 1, \dots, m)$$

Applying (1) and changing a summation index on the right,

$$\sum_{k,j} \beta_{ik} a_{kj} \xi_j = \sum_{l,j} \gamma_{il} \beta_{lj} \xi_j. \quad (i = 1, \dots, m)$$

Since this holds for arbitrary ξ_j 's, we have [see remark § 1]

$$\sum_{k=1}^m \beta_{ik} a_{kj} = \sum_{l=1}^m \gamma_{il} \beta_{lj}. \quad (i, j = 1, 2, \dots, m)$$

Hence

$$|\beta_{ik}| \cdot |a_{kj}| = |\gamma_{il}| \cdot |\beta_{lj}|$$

or

$$|a_{kj}| = |\gamma_{il}|.$$

6. Denote by $B_{\xi_r, \lambda \xi_s}$ the substitution

$$\xi_r' = \xi_r + \lambda \xi_s; \xi_i' = \xi_i, \quad (i = 1, \dots, m; i \neq r)$$

affecting only the index ξ_r . Its determinant is 1 if $r \neq s$, but is $1 + \lambda$ if $r = s$.

Theorem. *Every linear homogeneous substitution S can be placed under the form* BL , where B is derived from the $m(m-1)(p^n-1)$ substitutions*

$$B_{\xi_r, \lambda \xi_s}, \quad (r, s = 1, 2, \dots, m; r \neq s)$$

λ being any mark $\neq 0$ of the $GF[p^n]$, and where L is a substitution which leaves unchanged every index except the last which it multiplies by the determinant of S .

Let the given substitution S be

$$\xi_i' = \sum_{j=1}^m a_{ij} \xi_j. \quad (i = 1, 2, \dots, m)$$

Suppose

$$a_{1e} \neq 0, \quad a_{1j} = 0. \quad (j = 1, 2, \dots, e-1)$$

If $e > 1$, the substitution

$$T = \prod_{j=e}^m B_{\xi_1, a_{1j} \xi_j}$$

will replace ξ_1 by

$$\sum_{j=e}^m a_{1j} \xi_j = \sum_{j=1}^m a_{1j} \xi_j.$$

If $e = 1$, the substitution $T \equiv$

$$B_{\xi_1, a_{12} \xi_2} \cdot B_{\xi_2, \beta \xi_1} \cdot B_{\xi_1, \gamma \xi_2} \cdot \prod_{j=3}^m B_{\xi_1, a_{1j} \xi_j},$$

will accomplish the same result if

$$1 + \beta\gamma = a_{11}, \quad \gamma + a(1 + \beta\gamma) = a_{12},$$

which may be satisfied by any $\gamma \neq 0$, since $a_{11} \neq 0$.

We thus have $S = TS_1$, where S_1 is a new substitution which leaves ξ_1 unchanged and thus has the form

$$\xi_1' = \xi_1; \xi_i' = \sum_{j=1}^m \beta_{ij} \xi_j. \quad (i = 2, 3, \dots, m)$$

* The variation from Jordan, Art. 121, is due to the correction of l. 17, p. 94, where $S_1 T$ should read TS_1 .

To decompose S_1 , I build the substitution

$$T_1 = \prod_{i=2}^m B_{\xi_i, \gamma_i \xi_1}, \text{ viz.}$$

$$\xi_1' = \xi_1; \xi_i' = \xi_i + \gamma_i \xi_1, \quad (i = 2, 3, \dots, m)$$

where the γ_i 's are chosen later.

Denoting by S_2 the substitution

$$\xi_1' = \xi_1; \xi_i' = \sum_{j=2}^m \beta_{ij} \xi_j, \quad (i = 2, 3, \dots, m)$$

we will have $S_1 = T_1 S_2$ provided

$$\sum_{j=2}^m \beta_{ij} \gamma_j = \beta_{i1}. \quad (i = 2, 3, \dots, m)$$

But the γ_j 's can be determined so as to satisfy these equations since

$$|\beta_{ij}| = |S_1| = |S| \neq 0. \quad (i, j = 2, \dots, m)$$

Hence

$$S = T T_1 S_2.$$

Proceeding with S_2 as we did with S , etc.,

$$S = T T_1 \dots T_{2m-4} T_{2m-3} S_{2m-2},$$

where S_{2m-2} denotes the substitution

$$\xi_i' = \xi_i \quad (i = 1, 2, \dots, m-1); \xi_m' = |S| \cdot \xi_m.$$

7. Theorem. *If a linear homogeneous substitution S is commutative with all the $m(m-1)$ substitutions*

$$B_{\xi_k, \mu \xi_l}, \quad (k, l = 1, 2, \dots, m; k \neq l)$$

where μ is a fixed mark $\neq 0$ of the $GF[p^n]$, then S simply multiplies all the indices by the same mark.

Let the substitution S be

$$\xi_i' = \sum_{j=1}^m a_{ij} \xi_j. \quad (i = 1, 2, \dots, m)$$

We then find that $S \cdot B_{\xi_k, \mu \xi_l}$ and $B_{\xi_k, \mu \xi_l} \cdot S$ are respectively

$$\xi_k' = \sum_{j=1}^m (a_{kj} + \mu a_{lj}) \xi_j; \xi_i' = \sum_{j=1}^m a_{ij} \xi_j; \quad (i = 1, 2, \dots, m; i \neq k)$$

$$\xi_i' = \mu a_{ik} \xi_l + \sum_{j=1}^m a_{ij} \xi_j. \quad (i = 1, 2, \dots, m)$$

The conditions that the two expressions for ξ'_k shall be identical are, since $\mu \neq 0$,

$$a_{ll} = a_{kk}; a_{lj} = 0. \quad (j = 1, 2, \dots, m; j \neq l)$$

The conditions that the two expressions for ξ'_i ($i \neq k$) shall be identical are

$$a_{ik} = 0, \quad (i = 1, 2, \dots, m; i \neq k)$$

Since the two sets of conditions are to hold for k and $l = 1, 2, \dots, m$, $k \neq l$, S must be of the form

$$\xi'_i = a_{ii}\xi_i, \quad (i = 1, 2, \dots, m)$$

where $a_{11} = a_{22} = \dots = a_{mm}$.

Factors of composition of the generalized linear homogeneous group G of degree p^{nm} , §§ 8-12.*

8. Let $p^n - 1 = p_1 \cdot p_2 \cdot \dots \cdot p_k$, where $p_1, \dots, p_k$ are equal or different prime numbers. Let ρ be a primitive root of the equation

$$\xi^{p^n-1} - 1 = 0.$$

Denote by $G_{p_1}, G_{p_1 p_2}, \dots$ the sub-groups formed of those substitutions of G whose determinant is a power of $\rho^{p_1}, \rho^{p_1 p_2}, \dots$, respectively; finally, by $G_{p^n-1} \equiv \Gamma$ that formed by the substitutions of G having determinant unity.

Let d be the greatest common divisor of m and $p^n - 1$; $p'_1, p'_2, \dots, p'_i$ the prime factors, equal or different, of d ; ρ' a primitive root of

$$\xi^d - 1 = 0.$$

Denote by $H, H_{p'_1}, H_{p'_1 p'_2}, \dots$ the groups formed of those substitutions of Γ which multiply all the indices by the same power† of ρ' , by the same power of $\rho^{p'_1}, \dots$, respectively.

9. Theorem. *The factors of composition of G are*

$$p_1, p_2, \dots, p_k, \quad \frac{\Omega(m, n, p)}{d(p^n - 1)}, \quad p'_1, p'_2, \dots, p'_i,$$

except when $(m, n, p) = (2, 1, 2)$ or $(2, 1, 3)$.

* Some of the ideas used by Jordan in his decomposition of the linear group are to be found in a different form in the earlier work of Betti, l. c. vol. 3, pp 79-83, 1852, and vol. 6, p. 31, 1855. The latter shows that his group of degree p^v (see Section III) has as self-conjugate sub-group (of index 2) the group L of substitutions of determinant a square in the $GF[p^1]$; that L has as self-conjugate sub-group of order $p - 1$ the group of those substitutions which multiply all the indices by the same factor λ , a primitive root of p . He proves that in the case $p^v = 2^2$ or 3^2 all the factors of composition are prime [thus giving the exception in theorem § 9].

† If a substitution of Γ multiplies all the m indices by the mark μ , then $\mu^m = 1$, and hence $\mu^d = 1$. Thus μ is some power of ρ' .

It is clear from § 6 that the groups

$$G, G_{p_1}, G_{p_1 p_2}, \dots, \Gamma, H, H_{p'_1}, H_{p'_1 p'_2}, \dots, 1$$

have respectively the orders

$$\Omega(m, n, p), \frac{\Omega(m, n, p)}{p_1}, \frac{\Omega(m, n, p)}{p_1 p_2}, \dots, \frac{\Omega(m, n, p)}{p^n - 1}, d, \frac{d}{p'_1}, \frac{d}{p'_1 p'_2}, \dots, 1$$

and that each is a self-conjugate sub-group of the preceding. Further, the numbers p_i and p'_i being prime, there can be interpolated between G_{p_1} and $G_{p_1 p_2}$, for example, no new group which contains $G_{p_1 p_2}$ and is contained in G_{p_1} . It remains therefore to prove that, aside from the two exceptional cases, H is a *maximal* self-conjugate sub-group of Γ . To prove this we show that if a group I be self-conjugate under Γ and yet more general than H , then I will necessarily contain all the substitutions of Γ .

10. Let

$$\xi'_i = \sum_{j=1}^m a_{ij} \xi_j \quad (i = 1, \dots, m)$$

be a substitution S of I but not in H , which therefore does not multiply all the indices by the same factor. Then by § 7, S is not commutative with every $B_{\xi_1, \lambda \xi_2}$, λ being a *particular* mark $\neq 0$, e. g. $\lambda = 1$. To fix the ideas, suppose S is not commutative with $B_{\xi_1, \lambda \xi_2}$. The substitution

$$T = S^{-1} B_{\xi_1, \lambda \xi_2}^{-1} S B_{\xi_1, \lambda \xi_2}$$

will thus not reduce to the identity. Further T belongs to I ; for the transformed of S by $B_{\xi_1, \lambda \xi_2}$ belongs to I , since $B_{\xi_1, \lambda \xi_2}$ has the determinant unity and thus is in Γ .

To express the substitution T , we note that, for $i > 1$, $B_{\xi_1, \lambda \xi_2}$ leaves ξ_i unchanged; that S replaces ξ_i by $\sum_{j=1}^m a_{ij} \xi_j$, which $B_{\xi_1, \lambda \xi_2}^{-1}$ replaces by

$$\sum_{j=1}^m a_{ij} \xi_j - \lambda a_{i1} \xi_2,$$

which in turn S^{-1} replaces by $\xi_i - \lambda a_{i1} \varphi$, if φ denotes the linear function by which S^{-1} replaces ξ_2 . Thus T has the *form*

$$\xi'_1 = \sum_{j=1}^m \beta_{1j} \xi_j; \quad \xi'_i = \xi_i - \lambda a_{i1} \varphi \quad (i = 2, \dots, m)$$

where it is not necessary to determine the β_{ij} 's more closely. In this expression of T , which is the basis of the further developments, there is no longer any trace of the ξ_2 -specialization in $B_{\xi_1, \lambda \xi_2}$.

11. Let us first suppose that $m > 2$.

(1) Suppose $a_{i1} = 0$ ($i = 2, 3, \dots, m$). Then $\beta_{11} = 1$, the determinant of T being 1; while β_{ij} ($j = 2, \dots, m$) are not all zero, since T is not the identity. Let us take $\beta_{13} \neq 0$, changing if necessary the previous order of the independent indices $\xi_2, \xi_3, \dots, \xi_m$.

To simplify T we take a new system of independent indices η_i in place of the former ones ξ_i , viz

$$\eta_3 = \sum_{j=2}^m \beta_{1j} \xi_j; \quad \eta_i = \xi_i, \quad (i = 1, \dots, m; i \neq 3)$$

which is permissible since the determinant of transformation is $\beta_{13} \neq 0$. Then

$$\eta'_1 = \xi'_1 = \sum_{j=1}^m \beta_{1j} \xi_j = \beta_{11} \xi_1 + \sum_{j=2}^m \beta_{1j} \xi_j = \eta_1 + \eta_3.$$

$$\eta'_3 = \sum_{j=2}^m \beta_{1j} \xi'_j = \sum_{j=2}^m \beta_{1j} \xi_j = \eta_3.$$

$$\eta'_i = \xi'_i = \xi_i = \eta_i. \quad (i = 2, 4, 5, \dots, m)$$

Hence T becomes simply B_{η_1, η_3} . But by the Remark of § 5, I contains the substitution L (of determinant unity)

$$\eta'_1 = \lambda \eta_1; \quad \eta'_2 = \lambda^{-1} \eta_2; \quad \eta'_i = \eta_i, \quad (i = 3, \dots, m)$$

where λ is an arbitrary mark $\neq 0$ of the $GF[p^n]$. Hence I contains $L^{-1}TL$, i. e. $B_{\eta_1, \lambda \eta_3}$. Also I contains the substitution U_k of determinant unity,

$$\eta'_1 = \eta_k; \quad \eta'_k = \eta_1; \quad \eta'_2 = -\eta_2; \quad \eta'_i = \eta_i. \quad \left[\begin{array}{l} i = 3, 4, \dots, m \\ i \neq k, k > 2 \end{array} \right]$$

Hence I contains $U_k^{-1} B_{\eta_1, \lambda \eta_3} U_k$, which gives for $k = 3$ the substitution $B_{\eta_3, \lambda \eta_1}$ and for $k > 3$ the substitution $B_{\eta_k, \lambda \eta_3}$. Likewise I contains the transformed of these substitutions, etc., so that clearly I will contain all the substitutions

$$B_{\eta_i, \lambda \eta_k} \quad (i, k = 1, \dots, m; i \neq k)$$

But by § 6, these substitutions combine with each other to give every substitution of I , i. e. of determinant unity.

(2) If not every a_{i1} ($i = 2, 3, \dots, m$) is zero, suppose $a_{21} \neq 0$. Take $\eta_1, \eta_2, \dots, \eta_m$ as independent indices where

$$\eta_1 = \xi_1; \quad \eta_2 = \xi_2; \quad \eta_i = \xi_i - \frac{a_{i1}}{a_{21}} \xi_2, \quad (i = 3, 4, \dots, m)$$

the determinant of transformation being unity.

The $m - 2$ indices η_i ($i > 2$) are unchanged by T (of § 10); thus

$$\eta'_i = (\xi_i - \lambda a_{i1} \varphi) - \frac{a_{i1}}{a_{21}} (\xi_2 - \lambda a_{21} \varphi) = \xi_i - \frac{a_{i1}}{a_{21}} \xi_2 = \eta_i.$$

Hence the substitution T takes the form

$$\eta'_1 = \sum_{j=1}^m \gamma_{1j} \eta_j; \quad \eta'_2 = \sum_{j=1}^m \gamma_{2j} \eta_j; \quad \eta'_i = \eta_i \quad (i > 2),$$

where (by Remark of § 5) the determinant of T is

$$\gamma_{11} \gamma_{22} - \gamma_{12} \gamma_{21} = 1.$$

In this form of T the indices η_1, η_2 play the same role.

(2a) Suppose γ_{1i} and γ_{2i} ($i = 3, \dots, m$) are not all zero. Changing if necessary the order of $\eta_3, \eta_4, \dots, \eta_m$, we may suppose that γ_{13} and γ_{23} are not both zero.

The text in Jordan (l. c. p. 108, 1°) is here incorrect, but may be modified as follows, if our linear substitutions be on *four or more indices*:

T will contain the substitution

$$T_1 \equiv T^{-1} B_{\eta_3, \mu \eta_4}^{-1} T B_{\eta_3, \mu \eta_4},$$

(μ being an arbitrary mark $\neq 0$ of the $GF[p^n]$) viz

$$\eta'_1 = \eta_1 - \mu \gamma_{13} \eta_4; \quad \eta'_2 = \eta_2 - \mu \gamma_{23} \eta_4; \quad \eta'_i = \eta_i. \quad (i = 3, \dots, m)$$

Suppose for definiteness that $\gamma_{13} \neq 0$, and take $\omega_1, \dots, \omega_m$ as independent indices, where

$$\omega_1 = -\eta_1 / \gamma_{13}; \quad \omega_2 = \eta_2 - \gamma_{23} / \gamma_{13} \cdot \eta_1; \quad \omega_i = \eta_i. \quad (i = 3, \dots, m)$$

Then for the substitution T_1 we find

$$\omega'_1 = -\frac{\eta'_1}{\gamma_{13}} = -\frac{\eta_1 - \mu \gamma_{13} \eta_4}{\gamma_{13}} = \omega_1 + \mu \omega_4$$

$$\omega'_2 = \eta'_2 - \frac{\gamma_{23}}{\gamma_{13}} \eta'_1 = (\eta_2 - \mu \gamma_{23} \eta_4) - \left[\frac{\gamma_{23}}{\gamma_{13}} \eta_1 - \mu \gamma_{23} \eta_4 \right] = \omega_2.$$

$$\omega'_i = \eta'_i = \eta_i = \omega_i. \quad (i = 3, \dots, m)$$

Hence T_1 takes the form $B_{\omega_1, \mu \omega_4}$, which combined with its transformed by the substitutions of Γ will give as in (1) all the substitutions of Γ .

For the case of *three indices*,* I contains the substitutions

$$T_2 \equiv T^{-1} B_{\eta_1, \mu \eta_3}^{-1} T B_{\eta_1, \mu \eta_3} \text{ viz}$$

$$\eta_1' = \eta_1 - \mu(\gamma_{11} - 1)\eta_3; \eta_2' = \eta_2 - \mu\gamma_{21}\eta_3; \eta_3' = \eta_3.$$

$$T_3 \equiv T^{-1} B_{\eta_2, \mu \eta_3}^{-1} T B_{\eta_2, \mu \eta_3} \text{ viz}$$

$$\eta_1' = \eta_1 - \mu\gamma_{12}\eta_3; \eta_2' = \eta_2 - \mu(\gamma_{22} - 1)\eta_3; \eta_3' = \eta_3.$$

Now T_2 and T_3 are both of the form U :

$$\eta_1' = \eta_1 + \sigma_1\eta_3; \eta_2' = \eta_2 + \sigma_2\eta_3; \eta_3' = \eta_3.$$

If both T_2 and T_3 reduce to the identity, T becomes

$$\eta_1' = \eta_1 + \gamma_{13}\eta_3; \eta_2' = \eta_2 + \gamma_{23}\eta_3; \eta_3' = \eta_3,$$

which is of the form U . Hence in any case we have a substitution of the form U and not the identity. We then take $\omega_1, \omega_2, \omega_3$, defined above as independent indices and obtain for U the form B_{ω_1, ω_3} .

(2b) Suppose

$$\gamma_{1i} = \gamma_{2i} = 0. \quad (i = 3, \dots, m)$$

Since T does not reduce to the identity, we can not have simultaneously

$$\gamma_{11} = \gamma_{22} = 1, \quad \gamma_{12} = \gamma_{21} = 0.$$

Hence if we form T_2 and T_3 above for m indices, e. g. T_2 is

$$\eta_1' = \eta_1 - \mu(\gamma_{11} - 1)\eta_3; \eta_2' = \eta_2 - \mu\gamma_{21}\eta_3; \eta_i' = \eta_i \quad (i = 3, \dots, m)$$

we see that one of the two must not be the identity and we proceed as in (2a).

12. The case $m = 2$.

Let S be a substitution of I but not in H , which therefore does not multiply both indices by the same factor. Let η_1 be a function of the indices ξ_1 and ξ_2 which S does not multiply by a constant factor, e. g. $\eta_1 = \xi_1 + \xi_2$; let η_2 be the new function by which S replaces η_1 . Since η_1 and η_2 are linearly independent, we may take them as new indices, when S becomes (having determinant 1)

$$\eta_1' = \eta_2; \eta_2' = -\eta_1 + \delta\eta_2.$$

Now I contains the substitution T

$$\eta_1' = \alpha\eta_2; \eta_2' = -\alpha^{-1}\eta_1. \quad (\alpha \neq 0)$$

* M. Jordan was kind enough to send me a correction of the error above mentioned. His proof appears valid however only for three indices. It is given here with the usual modifications.

Hence I will contain $U \equiv T^{-1}STS$, viz

$$\eta_1' = -\alpha^{-2}\eta_1; \eta_2' = -\delta(1 + \alpha^{-2})\eta_1 - \alpha^2\eta_2.$$

(1) Suppose $\delta \neq 0$.

Then I will contain U^2 , which for $\alpha = 1$ becomes

$$\eta_1' = \eta_1; \eta_2' = 4\delta\eta_1 + \eta_2.$$

If $p > 2$, we can replace η_1 by another index

$$\Phi = 4\delta\eta_1.$$

Then U^2 becomes $B_{\eta_2, \Phi}$. But I contains the substitution V ,

$$\Phi' = \eta_2; \eta_2' = -\Phi.$$

Thus I contains $V^{-1}U^2V$ or $B_{\Phi, -\eta_2}$.

If L denote the substitution belonging to I

$$\Phi' = \lambda^{-1}\Phi; \eta_2' = \lambda\eta_2, \quad (\lambda = \text{any mark} \neq 0)$$

I will contain the substitution $L^{-1}B_{\eta_2, \Phi}L$ or $B_{\eta_2, \lambda^2\Phi}$.

By virtue of the property

$$B_{\eta_2, \lambda_1^2\Phi} \cdot B_{\eta_2, \lambda_2^2\Phi} = B_{\eta_2, (\lambda_1^2 + \lambda_2^2)\Phi}$$

we must reach a substitution $B_{\eta_2, \nu\Phi}$, where ν is a not-square in the $GF[p^n]$, p being > 2 by hypothesis. For, if not, the totality of the $(p^n - 1)/2$ squares in the $GF[p^n]$, together with the mark zero, would form not only a multiplicative but also an *additive* group and therefore* a Galois field of order say $p^{n'}$ included in the $GF[p^n]$. But $p' = p$, quâ additive period of every mark $\neq 0$. Thus

$$(p^n - 1)/2 + 1 = p^{n'},$$

which is impossible.

Having one, we reach every not-square by the formula

$$L^{-1}B_{\eta_2, \nu\Phi}L \equiv B_{\eta_2, \lambda^2\nu\Phi}.$$

Thus for $\delta \neq 0$ and $p > 2$, I will contain all the substitutions $B_{\eta_2, \mu\Phi}$ and $B_{\Phi, \mu\eta_2}$, μ being an arbitrary mark $\neq 0$ of the $GF[p^n]$, and hence all the substitutions of I .

(2) Suppose $\delta = 0$.

(2a) If $p^n = 2^2$ or if $p^n > 5$, we can find a mark $\alpha \neq 0$ of the $GF[p^n]$ such that $\alpha^4 \neq 1$ and then a mark β such that

$$\beta(\alpha^4 - 1) = \mu = \text{any mark} \neq 0.$$

* Moore, l. c. § 40.

Then I contains the substitution

$$B_{\eta_1, \beta\eta_2}^{-1} U B_{\eta_1, \beta\eta_2} U^{-1}, \text{ viz }$$

$$\gamma_1' = \gamma_1 - \beta(\alpha^4 - 1)\gamma_2; \gamma_2' = \gamma_2,$$

or $B_{\eta_1, \mu\eta_2}$, which combined with its transformed by the substitutions of I will produce I .

(2b) If $p^n = 5$, we may take as independent indices

$$\omega_1 = 2\gamma_1 + \gamma_2; \omega_2 = -2\gamma_1 + \gamma_2.$$

Then S will become

$$\omega_1' = 2\omega_1; \omega_2' = -2\omega_2.$$

Thus I contains the substitution

$$SB_{\omega_1, \omega_2}^{-1} S^{-1} B_{\omega_1, \omega_2} = B_{\omega_1, 2\omega_2}$$

and hence also its cube B_{ω_1, ω_2} .

(2c) For $p^n = 2$, the linear homogeneous group on two indices has the order $(2^2 - 1)(2^2 - 2) = 6$. It contains a subgroup of order 3 formed of the powers of the substitution

$$\xi_1' = \xi_2; \xi_2' = \xi_1 + \xi_2$$

which represents the literal substitution $(l_{00})(l_{01}l_{10})$. The index of this subgroup being 2, it is self-conjugate. The factors of composition are thus 2 and 3.

(2d) For $p^n = 3$, we may prove that the $(3^2 - 1)(3^2 - 3) = 48$ substitutions of the linear homogeneous group G of degree 9 are derived from

$$\begin{aligned} \text{(A)} \quad & \xi_1' = -\xi_1; \quad \xi_2' = \xi_1 + \xi_2. \\ \text{(B)} \quad & \xi_1' = \xi_2; \quad \xi_2' = -\xi_1 + \xi_2. \\ \text{(C)} \quad & \xi_1' = -\xi_2; \quad \xi_2' = \xi_1. \\ \text{(D)} \quad & \xi_1' = \xi_1 + \xi_2; \quad \xi_2' = \xi_1 - \xi_2. \\ \text{(E)} \quad & \xi_1' = -\xi_1; \quad \xi_2' = -\xi_2. \end{aligned}$$

Thus for the groups

$$\{E\}, \{E, D\}, \{E, D, C\}, \{E, D, C, B\}, \{E, D, C, B, A\} = G$$

we may verify the following generating relations :

$$E^2 = 1 .$$

$$D^2 = E ; DE = ED .$$

$$C^2 = E ; CE = EC ; CD = EDC .$$

$$B^3 = E ; BE = EB ; BD = CDB ; BC = DB .$$

$$A^2 = 1 ; AE = EA ; AD = CA ; AC = DA ; AB = ECB^2A .$$

From these relations it follows at once that the above groups have for orders 2, 4, 8, 24, 48, respectively, and that each is a self-conjugate subgroup of the following. Hence the factors of composition of G are 2, 3, 2, 2, 2.

13. Since the quotient-group* of any two consecutive groups in the series of composition of any group is a simple group, we have the result that I/H is a simple group of order

$$\frac{\Omega(m, n, p)}{d(p^n - 1)} = \frac{(p^{nm} - 1)(p^{nm} - p^n) \dots (p^{nm} - p^{nm-n})}{d(p^n - 1)}$$

except in the cases $(m, n, p) = (2, 1, 2)$ and $(2, 1, 3)$.

Compare section II.

SECTION II.—*Linear Fractional Group*.†

14. In our generalized linear homogeneous group G of degree p^{nm} on m indices, let us class into the same system the $p^n - 1$ letters

$$l_{\mu \bar{\xi}_1, \mu \bar{\xi}_2, \dots, \mu \bar{\xi}_m}$$

where the $\bar{\xi}_i$'s are fixed but μ runs through all the marks except zero of the $GF[p^n]$, or, otherwise expressed, the $p^n - 1$ letters corresponding to the same values of the ratios $\bar{\xi}_i/\bar{\xi}_m$ ($i = 1, 2, \dots, m - 1$).

Each substitution of G will replace the letters of any one system by letters all of some one system. We have thus $(p^{nm} - 1)/(p^n - 1)$ systems, whose displacements (by the substitutions of G) form a group H of degree $(p^{nm} - 1)/(p^n - 1)$. But there are exactly $p^n - 1$ substitutions of G which do not displace any system, viz,

$$\xi'_i = \mu \bar{\xi}_i . \quad \left[\begin{array}{l} i = 1, 2, \dots, m \\ \mu = \text{any mark} \neq 0 \end{array} \right]$$

* Hölder, *Mathematische Annalen*, vol. 34.

† Compare Jordan, l. c. Arts. 315-317 ; Betti, l. c. vol. 3, p. 74, 1852.

The substitutions of H may be exhibited thus :

$$\xi_1' : \xi_2' : \dots : \xi_m' = \sum_{j=1}^m a_{1j} \xi_j : \sum_{j=1}^m a_{2j} \xi_j : \dots : \sum_{j=1}^m a_{mj} \xi_j .$$

The order of H , being the total number $\mathcal{Q}(m, n, p)$ of the substitutions in G divided by the number of those leaving the systems invariant, is thus $\mathcal{Q}(m, n, p)/(p^n - 1)$.

15. The linear fractional group H is clearly meriedrically isomorphic with the linear homogeneous group G . To the subgroup G' formed of those substitutions of G whose determinant is unity there corresponds a subgroup H' formed of those substitutions of H whose determinant is unity, or, as is equivalent, whose determinant is any m th power in the $GF[p^n]$. For the substitutions of H remain unchanged by multiplying the m homogeneous indices by the same mark μ , which multiplies the determinant by μ^m .

Let d be the greatest common divisor of m and $p^n - 1$. Then* the proportion of marks (excluding zero) of the $GF[p^n]$ which are m th powers is $1:d$. Hence the order of H' is $\mathcal{Q}(m, n, p)/d(p^n - 1)$.

Now,† the maximal self-conjugate subgroup of G' is, for $(m, n, p) \neq (2, 1, 2)$ or $(2, 1, 3)$, the group of substitutions which multiplies every index by the same mark. The subgroup of H' isomorphic with it is evidently 1. Hence the group H' of the linear fractional substitutions on $m - 1$ indices having determinant unity (or any m th power) is a *simple* group of degree $(p^{nm} - 1)/(p^n - 1)$ and order $\mathcal{Q}(m, n, p)/d(p^n - 1)$, with the two exceptions $(m, n, p) = (2, 1, 2)$ and $(2, 1, 3)$.

16. The triply-infinite system of simple groups thus reached affords a direct generalization of the doubly-infinite system obtained‡ differently,

$$\frac{1}{2} p^n (p^{2n} - 1), \quad p > 2, \quad (p, n) \neq (3, 1).$$

$$p^n (p^{2n} - 1), \quad p = 2, \quad (p, n) \neq (2, 1).$$

* Proof. A mark $\mu \neq 0$ is an m th power in the $GF[p^n]$ if and only if

$$\mu^{(p^n - 1)/m} = 1. \quad (1)$$

By raising (1) to the power m/d , we find a necessary condition,

$$\mu^{(p^n - 1)/d} = 1. \quad (2)$$

But the condition (2) is sufficient. For, m/d being prime to $p^n - 1$, the extraction in the $GF[p^n]$ of the root m/d is (by Part I, § 18) always possible and indeed uniquely. Hence from (2) we derive (1). Thus the $(p^n - 1)/d$ marks satisfying (2) [cf. Moore, l. c. § 32] give the m th powers in the $GF[p^n]$.

† Section I, §§ 8-12.

‡ E. H. Moore, *A doubly-infinite system of simple groups*, *Bulletin of the New York Mathematical Society*, vol. 3, pp. 73-78, 1894.

Thus

$$\frac{\Omega(2, n, p)}{d(p^n - 1)} = \frac{(p^{2n} - 1)(p^{2n} - p^n)}{d(p^n - 1)} = \frac{p^n(p^{2n} - 1)}{d},$$

where d is the greatest common divisor of 2 and $p^n - 1$.

17. Our triply-infinite system of simple groups yields exactly 13 having an order $< 10,000$, viz :*

$$\begin{aligned} 60 &= ((2, 1, 5)) = ((2, 2, 2)) = \tfrac{1}{2} \cdot 5! \\ 168 &= ((2, 1, 7)) = ((3, 1, 2)) . \\ 360 &= ((2, 2, 3)) = \tfrac{1}{2} \cdot 6! \\ 504 &= ((2, 3, 2)) . \\ 660 &= ((2, 1, 11)) . \\ 1092 &= ((2, 1, 13)) . \\ 2448 &= ((2, 1, 17)) . \\ 3420 &= ((2, 1, 19)) . \\ 4080 &= ((2, 4, 2)) . \\ 5616 &= ((3, 1, 3)) . \\ 6072 &= ((2, 1, 23)) . \\ 7800 &= ((2, 2, 5)) . \\ 9828 &= ((2, 3, 3)) . \end{aligned}$$

The simple group of order $\tfrac{1}{2} \cdot 7! = 2520$ is not found in this list. Of interest is that of order

$$20160 = ((4, 1, 2)) = ((3, 2, 2)) = \tfrac{1}{2} \cdot 8!$$

By noting that the number $\Omega(m, n, p)/d(p^n - 1)$ contains the factor p exactly to the power $nm(m-1)/2$, we may prove that $\tfrac{1}{2} \cdot N!$ is not of the form $((m, n, p))$ for $8 < n < 16$.

Thus for $N = 9$, $\tfrac{1}{2} \cdot 9! = 2^6 \cdot 3^4 \cdot 5 \cdot 7$. Evidently $p \neq 5, \neq 7$, since then $m = 2, n = 1$. If $p = 3$, then $nm(m-1)/2 = 4$, so that $m = 2, n = 4$; while $((2, 4, 3)) = 2^4 \cdot 3^4 \cdot 5 \cdot 41$. Lastly $p = 2$ leads to the possibilities $((4, 1, 2))$, $((3, 2, 2))$ and $((2, 6, 2))$ all of which are excluded.

Analogously, we may verify that the numbers $((3, 2, 3)) = 2^7 \cdot 3^6 \cdot 5 \cdot 7 \cdot 13$, $((3, 3, 2)) = 2^9 \cdot 3^2 \cdot 7^2 \cdot 73$, $((3, 3, 3)) = 2^4 \cdot 3^9 \cdot 13^2 \cdot 7 \cdot 757$, $((4, 2, 2)) =$

* $((m, n, p))$ is used as an abbreviation for $\Omega(m, n, p)/d(p^n - 1)$.

$2^{12} \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 17$, and $((4, 2, 3)) = 2^{10} \cdot 3^{12} \cdot 5^2 \cdot 7 \cdot 13 \cdot 41$, are each given but once in the form $((m, n, p))$.

It follows that the system of simple groups of order $((m, n, p))$ reached in this paper includes simple groups not in Jordan's system ($n = 1$) and not in Moore's system ($m = 2$).

SECTION III.—*The Betti-Mathieu Group.*

Identification with Jordan's Linear Group, §§ 18–20.

18. It was shown in Part I, §§ 58–59, that the quantic

$$F(X) = \sum_{i=1}^m A_i X^{p^{n(m-i)}},$$

belonging to the $GF[p^{nm}]$, represents a substitution on its p^{nm} marks if and only if

$$\begin{vmatrix} A_1 & A_2 & \dots & A_m \\ A_2^{p^n} & A_3^{p^n} & \dots & A_1^{p^n} \\ \dots & \dots & \dots & \dots \\ A_m^{p^{n(m-1)}} & A_1^{p^{n(m-1)}} & \dots & A_{m-1}^{p^{n(m-1)}} \end{vmatrix} \neq 0.$$

Let R be a primitive root of the $GF[p^{nm}]$, thus satisfying an equation of degree m belonging to and irreducible in the $GF[p^n]$. Then any mark X of the $GF[p^{nm}]$ may be expressed in the form

$$X = \sum_{i=1}^{m-1} \tilde{\xi}_i R^i$$

where the $\tilde{\xi}_i$'s are marks of the $GF[p^n]$.

If we thus express A_i , X and X' in the substitution

$$X' = \sum_{i=1}^m A_i X^{p^{n(m-i)}} \quad (1)$$

and reduce the powers of R to a degree $\leq m - 1$ by means of our irreducible equation, we may equate coefficients of like powers of R . Since

$$\tilde{\xi}_i^{p^n} = \tilde{\xi}_i$$

we evidently have a linear substitution on m indices

$$\tilde{\xi}_i' = \sum_{j=0}^{m-1} a_{ij} \tilde{\xi}_j \quad (i = 0, 1, \dots, m-1) \quad (2)$$

where the ξ_i 's and the a_{ij} 's belong to the $GF[p^n]$.

19. *Inversely, every such substitution (2) on the marks of the $GF[p^n]$ can be represented in the form (1).*

It is sufficient to prove that a set of marks $A_1, A_2, \dots, A_m$ in the $GF[p^{nm}]$ may be found such that (1) will transform any given set of m marks of the $GF[p^{nm}]$ linearly independent in the $GF[p^n]$, as

$$1, R, R^2, \dots, R^{m-1}$$

into any other such set of m linearly independent marks,

$$B_i = \sum_{j=0}^{m-1} \beta_{ij} R^j \quad (i = 0, \dots, m-1)$$

where thus we have, $\beta_{ij} \neq 0$. For then on account of the property of $F(X)$,

$$F(\lambda_1 X_1 + \lambda_2 X_2 + \dots + \lambda_t X_t) = \lambda_1 F(X_1) + \lambda_2 F(X_2) + \dots + \lambda_t F(X_t),$$

the p^{nm} marks $\sum_{i=0}^{m-1} \lambda_i R^i$ of the $GF[p^{nm}]$ will be transformed into the marks $\sum_{i=0}^{m-1} \lambda_i B_i$ all distinct.

Now the conditions on the A_i 's for the above transformation are

$$\sum_{i=1}^m A_i (R^k)^{p^{n(m-i)}} = B_k, \quad (k = 0, 1, \dots, m-1)$$

which may be solved in the field for A_i since the determinant in R is $\neq 0$ [see Part I, § 57, (7)].

This theorem may be shown indirectly thus. Generalizing the work both of Betti* and Jordan,† we may prove that the maximum group commutative with (i. e. the group of transformation into itself of) the group

$$G_p^{p^{nm}} = \{X' = X + C\} = \{\xi'_i = \xi_i + a_i \ (i = 0, \dots, m-1)\}$$

is on the one hand

$$\{X' = \sum_{i=1}^m A_i X^{p^{n(m-i)}} + B\}$$

and on the other

$$\{\xi'_i = \sum_{j=0}^{m-1} a_{ij} \xi_j + \beta_i \ (i = 0, 1, \dots, m-1)\}.$$

* Betti, l. c. vol. 3, pp. 72-73, 1852, and vol. 6, p. 26, 1855.

† Jordan, l. c. Arts. 118-119.

20. *Order* of the Betti-Mathieu group.* If as in § 18 we express X of the substitution (1) in terms of R , we have

$$X' = \sum_{j=0}^{m-1} \Gamma_j \xi_j$$

where

$$\Gamma_j = \sum_{i=1}^m A_i R_i^{j \cdot p^{i(m-1)}}.$$

But if (1) is indeed a substitution, then by § 57 of Part I, X' is zero if and only if $X = 0$, i. e. if $\xi_0 = \xi_1 = \dots = \xi_{m-1} = 0$. Hence the necessary and sufficient condition that (1) shall be a substitution on the marks of the $GF[p^{nm}]$ is that $\Gamma_0, \Gamma_1, \dots, \Gamma_{m-1}$ be linearly independent in the $GF[p^n]$.

To give a more direct proof, let $\Gamma_0, \Gamma_1, \dots, \Gamma_{m-1}$ be a particular set of m marks. Then $\xi_0 \Gamma_0$ takes p^n values; $\xi_0 \Gamma_0 + \xi_1 \Gamma_1$ takes p^{2n} values if and only if

$$\Gamma_1 \neq \mu \Gamma_0$$

for any mark μ in the $GF[p^n]$. Finally, $\sum_{j=0}^{m-1} \Gamma_j \xi_j$ takes the required number of values p^{nm} if and only if (for $k = 1, 2, \dots, m-1$)

$$\Gamma_k \neq \sum_{j=0}^{k-1} \mu_j \Gamma_j,$$

for any set of marks $\mu_0, \mu_1, \dots, \mu_{k-1}$ in the $GF[p^n]$.

We may now readily enumerate the substitutions (1). Γ_0 may be chosen in $p^{nm} - 1$ ways, the value $\Gamma_0 = 0$ being excluded since then $X' = 0$ when $X = 1$. After a definite choice of Γ_0 , we may take Γ_1 in $p^{nm} - p^n$ ways, etc.; finally Γ_{m-1} in $p^{nm} - p^{n(m-1)}$ ways. Hence the number of substitutions is

$$\Omega(m, n, p) = (p^{nm} - 1)(p^{nm} - p^n)(p^{nm} - p^{2n}) \dots (p^{nm} - p^{n(m-m)}).$$

Mathieu's special type of substitution, §§ 21-24.

21. Mathieu states in general (l. c. vol. 6, p. 304) and proves for the case $n = 1$ (pp. 294-300) the theorem that from the substitutions, belonging to the $GF[p^{nm}]$,

$$Z' = Z + A \sum_{i=0}^{m-1} (HZ)^{p^{ni}} \quad (2)$$

all the substitutions (1) of the Betti-Mathieu group may be derived.

22. The condition that (2) shall represent a substitution on the marks of

* Betti, l. c. vol. 6, pp. 13 and 27, 1855; Mathieu, l. c. vol. 6, pp. 282-5 and 302-3.

the $GF[p^{nm}]$ is, writing the columns of the determinant of § 18 in reverse order, that

$$\begin{vmatrix} AH + 1, & AH^{p^n}, & AH^{p^{2n}}, & \dots, & AH^{p^{n(m-1)}} \\ A^{p^n}H, & A^{p^n}H^{p^n} + 1, & A^{p^n}H^{p^{2n}}, & \dots, & A^{p^n}H^{p^{n(m-1)}} \\ A^{p^{2n}}H, & A^{p^{2n}}H^{p^n}, & A^{p^{2n}}H^{p^{2n}} + 1, & \dots, & A^{p^{2n}}H^{p^{n(m-1)}} \\ \dots & \dots & \dots & \dots & \dots \\ A^{p^{n(m-1)}}H, & A^{p^{n(m-1)}}H^{p^n}, & A^{p^{n(m-1)}}H^{p^{2n}}, & \dots, & A^{p^{n(m-1)}}H^{p^{n(m-1)}} + 1 \end{vmatrix}$$

shall not vanish. Multiplying the i th column by $H^{p^{ni} - p^{n(i-1)}}$ and subtracting from the $i + 1$ st this becomes

$$\begin{vmatrix} AH + 1, & -H^{p^{n-1}}, & 0, & \dots, & 0, & 0 \\ A^{p^n}H, & 1, & -H^{p^{2n} - p^n}, & \dots, & 0, & 0 \\ A^{p^{2n}}H, & 0, & 1, & \dots, & 0, & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ A^{p^{n(m-2)}}H, & 0, & 0, & \dots, & 1, & -H^{p^{n(m-1)} - p^{n(m-2)}} \\ A^{p^{n(m-1)}}H, & 0, & 0, & \dots, & 0, & 1 \end{vmatrix}.$$

Expanding with respect to the elements of the first column, the first minor of $A^{p^{nk}}H$ is

$$(-1)^k H^{p^{nk} - p^{n(k-1)}} \cdot H^{p^{n(k-1)} - p^{n(k-2)}} \dots H^{p^{n-1}} = (-1)^k H^{p^{nk} - 1},$$

given by the product of the terms in H just above the main diagonal as far as the k th row and the terms 1 in the main diagonal beginning with the $(k + 2)$ th row. The condition is thus

$$\sum_{k=0}^{m-1} (AH)^{p^{nk}} + 1 \neq 0.$$

We may derive this condition directly from the decomposition

$$H(Z^{p^{nm}} - Z) = \prod_{j=0}^{p^n-1} \left\{ \sum_{i=0}^{m-1} (HZ)^{p^{ni}} + a_j \right\}$$

where α_j runs through all the marks of the $GF[p^n]$. Thus any mark M of the $GF[p^{nm}]$ satisfies an equation of the form

$$\sum_{i=0}^{m-1} (HZ)^{p^{ni}} = \alpha_M$$

where α_M is a suitably chosen mark of the $GF[p^n]$.

We seek the condition under which

$$Z + A \sum_{i=0}^{m-1} (HZ)^{p^{ni}} = 0$$

has no solution except $Z = 0$ in the $GF[p^{nm}]$. But if it has a solution $Z_0 \neq 0$, then

$$\sum_{i=0}^{m-1} (HZ_0)^{p^{ni}} = \alpha_{Z_0} \neq 0.$$

Hence

$$Z_0 + A \alpha_{Z_0} = 0,$$

so that

$$\sum_{i=0}^{m-1} (-\alpha_{Z_0} HA)^{p^{ni}} = \alpha_{Z_0} \sum_{i=0}^{m-1} (-HA)^{p^{ni}} = \alpha_{Z_0}.$$

Hence

$$\sum_{i=0}^{m-1} (-HA)^{p^{ni}} = 1.$$

23. $F(Z) = \sum_{i=0}^{m-1} (HZ)^{p^{ni}}$ has the properties in the $GF[p^{nm}]$

$$F(Z_1 + Z_2) = F(Z_1) + F(Z_2).$$

$$[F(Z)]^{p^n} = F(Z).$$

$$F[M \cdot F(Z)] = F(M) \cdot F(Z).$$

Hence the result of applying first the substitution

$$Z' = Z + A \cdot F(Z) \tag{2}$$

and afterwards the substitution

$$Z' = Z + B \cdot F(Z)$$

is the same as applying the single substitution

$$Z' = Z + \{A + B + A \cdot F(B)\} \cdot F(Z). \tag{3}$$

Thus the square of the substitution (2) is

$$Z' = Z + A \{2 + F(A)\} F(Z).$$

Using (3) we have by induction that the k th power of (2) is

$$Z' = Z + \frac{[1 + F(A)]^k - 1}{F(A)} A \cdot F(Z).$$

24. The substitution (2) leaves unchanged the $p^{n(m-1)}$ letters whose indices satisfy the equation

$$\sum_{i=0}^{m-1} (HZ)^{p^{ni}} = 0.$$

If $F(A) = 0$, the k th power of (2) reduces to

$$Z' = Z + kA \cdot F(Z),$$

when (2) is a regular substitution on $p^{nm} - p^{nm-n}$ letters composed of cycles of p letters.

If $F(A) = a_A \pm 1$, a_A being a mark $\neq 0$ of the $GF[p^n]$ and if e is the least integer such that

$$\{1 + F(A)\}^e = 1,$$

(2) represents a regular substitution on $p^{nm} - p^{nm-n}$ letters composed of cycles of e letters.

The substitutions (2) constitute the totality of those substitutions (1) which affect only $p^{nm} - p^{nm-n}$ letters (Mathieu, l. c. vol. 6, p. 288).

UNIVERSITY OF CHICAGO, April 27, 1896.

ERRATA.

Page 68, line 8, read $(p - s + 1)/2$; line 9, read *shall not*.

Page 71, line 5 from bottom, read C_{ij} .

Page 73, line 10, for yl_p read y_{lp} .

Page 81, line 19, for C_5^{5m+4} read C_5^{m+4} .

Page 84, note, read *Arithmeticae*.

Page 89, line 2, for 7δ read 7γ .

Page 90, line 12, for $a_2^2 a_3^3$ read $a_2^2 a_3^2$.

Page 91, bottom, for p^{2n-1} read $p^{2n} - 1$.

Page 94, middle, read $X^{p^{n(m-1)}-1}$.

Page 95, equation (5), for j^i read j, i .

Page 100, bottom, for a_{k+2} read a_{k+1} .

Page 102, line 19, for $n + 1$ read $n - 1$.

Page 103, bottom, for $\frac{1}{2} a_2^2 a_6^6$ read $\frac{1}{2} a_2^2 a_6$.

Page 104, line 9, read $\xi^{2(7^n-1)}$.

Page 110, line 12, read $\xi^5 \pm 2\xi^2$.

Page 112, line 12, for $a_2^6 a_5^5$ read $a_2^6 a_5^3$.

Page 117, line 1, read §§ 83-86; line 23, for (1_3) read (1_3) ; line 26, for (1_3) read (1) .

Page 118, line 8, read $GF[2^n]$; line 10, for 73 read > 3 .

